개발자 가이드

AWS Config

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Config: 개발자 가이드

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

란 무엇입니까 AWS Config? 1
고려 사항 1
사용 방법 AWS Config 1
리소스 관리 1
감사, 보안 및 규정 준수 2
구성 변경 관리 및 문제 해결 2
보안 분석 2
파트너 솔루션 2
Features 3
AWS Config 작동 방식 4
리소스 검색 4
리소스 추적 5
구성 항목 전송 5
에 대한 액세스 제어 AWS Config 8
용어 및 개념 8
AWS Config 인터페이스 10
리소스 관리 10
구성 레코더 11
전송 채널 5
AWS Config 규칙 12
적합성 팩 15
집계자 16
AWS 서비스 통합 17
AWS Organizations 17
AWS Control Tower 17
AWS CloudTrail 17
AWS Security Hub 18
AWS Trusted Advisor 18
AWS Audit Manager 19
AWS Systems Manager 19
AWS Firewall Manager 19
Amazon EC2 전용 호스트 20
Application Load Balancers 20
AWS CodeBuild 20

AWS X-Ray 20
AWS Service Management Connector 21
Amazon API Gateway 21
리전 지원 21
고려 사항 21
지원되는 리전 목록 22
서비스 한도 26
추가 정보 28
AWS 용 소프트웨어 개발 키트 AWS Config 29
시작하기 30
에 가입 AWS 30
에 가입 AWS 계정 30
관리자 액세스 권한이 있는 사용자 생성 30
를 시작하는 방법 AWS Config 32
설정(콘솔) 32
설정 32
원클릭 설정 33
수동 설정 36
설정(AWS CLI) 42
설정 42
사전 조건 42
시작 AWS Config 106
설정 확인 109
AWS SDKs 작업 111
구성 레코더 113
고객 관리형 구성 레코더에 대한 고려 사항 113
서비스 연결 구성 레코더에 대한 고려 사항 114
지원되는 서비스 115
구성 레코더에 대한 드리프트 감지 116
고객 관리형 구성 레코더 시작 116
고객 관리형 구성 레코더 중지 116
고객 관리형 구성 레코더의 레코딩 빈도 변경 117
고객 관리형 구성 레코더 이름 바꾸기 120
구성 레코더 보기 121
구성 레코더 삭제 122
전송 채널 124

고려 사항 124
용어 125
구성 항목의 구성 요소 126
전송 채널 보기 127
전송 채널 업데이트 128
전송 채널의 이름 바꾸기 132
구성 스냅샷 전송 133
구성 스냅샷 전송 134
전송 상태 확인 134
구성 스냅샷 확인 135
구성 스냅샷 확인 135
구성 스냅샷 예시 135
알림 예제 141
구성 항목 변경 알림의 예시 142
구성 기록 전달 알림 예 157
구성 스냅샷 전달 시작 알림 예 157
구성 스냅샷 전달 알림 예 158
준수 변경 알림 예 159
규칙 평가 시작 알림 예 163
크기를 초과한 구성 항목 변경 알림 예 164
전달 실패 알림 예 167
AWS Config 대시보드 169
규정 준수 및 리소스 인벤토리 169
AWS Config 사용량 및 성공 지표 171
리소스 관리 173
지원되는 리소스 유형 174
Amazon 앱Stream 175
Amazon AppFlow 175
..... 175
Amazon API Gateway 176
Amazon Athena 177
Amazon Bedrock 177
Amazon CloudFront 177
Amazon CloudWatch 178
Amazon CodeGuru 179
Amazon Cognito 179

Amazon Connect 180
Amazon Detective 180
Amazon DynamoDB 181
Amazon EC2 181
Amazon ECR 190
Amazon ECS 190
Amazon EFS 191
Amazon EKS 191
Amazon EMR 192
Amazon EventBridge 192
Amazon Forecast 193
Amazon Fraud Detector 194
Amazon GuardDuty 194
Amazon Inspector 195
Amazon IVS 195
Amazon Keyspaces 195
Amazon OpenSearch Service 196
Amazon Personalize 197
Amazon Pinpoint 197
Amazon QLDB 198
Amazon Kendra 198
Amazon Kinesis 199
Amazon Lex 199
Amazon Lightsail 200
Amazon Lookout for Metrics 200
Amazon Lookout for Vision 201
Amazon Macie 201
Amazon Managed Grafana 201
Amazon Managed Service for Prometheus 201
Amazon MemoryDB 202
Amazon MQ 202
Amazon MSK 202
Amazon QuickSight 203
Amazon Redshift 203
Amazon RDS 205
Amazon Route 53 206

Amazon SageMaker AI 207
Amazon SES 209
Amazon SNS 209
Amazon SQS 209
Amazon S3 210
Amazon WorkSpaces 212
AWS Amplify 212
AWS AppConfig 212
AWS App Runner 213
AWS App Mesh 214
AWS AppSync 214
AWS Audit Manager 215
AWS Auto Scaling 215
AWS Backup 216
AWS Batch 217
AWS Budgets 217
AWS Certificate Manager 217
AWS CloudFormation 218
AWS CloudTrail 218
AWS Cloud9 218
AWS Cloud Map 219
AWS CodeArtifact 219
AWS CodeBuild 220
AWS CodeDeploy 220
AWS CodePipeline 221
AWS Config 221
AWS DMS 222
AWS DataSync 223
AWS Device Farm 224
AWS Elastic Beanstalk 225
AWS FIS 225
AWS Global Accelerator 226
AWS Glue 226
AWS Ground Station 227
AWS HealthLake 227
AWS IAM 227

AWS IoT 229
AWS KMS 232
AWS Lambda 233
AWS Mainframe Modernization 233
AWS Network Firewall 233
AWS Network Manager 234
AWS Panorama 235
AWS Private CA 236
AWS Resilience Hub 236
AWS 리소스 탐색기 236
AWS RoboMaker 237
AWS Signer 237
AWS Secrets Manager 237
AWS Security Hub 238
AWS Service Catalog 238
AWS Shield 238
AWS Step Functions 239
AWS Systems Manager 239
AWS Transfer Family 240
AWS WAF 241
AWS X-Ray 243
Elastic Load Balancing 243
MediaConnect 244
MediaPackage 244
MediaTailor 245
리전 가용성별 리소스 범위 245
북아메리카 및 남아메리카 245
유럽 300
아시아 태평양 346
중국 427
아프리카 및 중동 446
GovCloud 473
AWS 리소스 기록 496
고려 사항 497
리전 및 글로벌 리소스 497
AWS Config 규칙 및 글로벌 리소스 유형 501

레코딩 빈도 ... 502
기록되지 않은 리소스 ... 503
리소스 기록(콘솔) ... 503
리소스 기록(AWS CLI) ... 507
리소스 제외 ... 514
레코딩 중지 ... 515
타사 리소스 레코딩(AWS CLI) ... 515
리소스 추가 ... 516
구성 항목 레코딩 ... 519
구성 항목 읽기 ... 520
리소스 삭제 ... 521
소프트웨어 구성 레코딩 ... 522
사전 조건 ... 522
소프트웨어 구성 레코딩 ... 523
리소스 조회 ... 524
리소스 확인 ... 526
규정 준수 상태 보기(콘솔) ... 526
규정 준수(AWS SDKs) 보기 ... 527
규정 준수 이력 보기 ... 533
규정 준수 이력 보기(콘솔) ... 533
규정 준수 이력 보기(AWS CLI) ... 533
리소스 및 규칙 ... 539
규정 준수 이력 쿼리 ... 540
리소스에 태그 지정 ... 541
태그 지정에 관련된 제한 ... 542
AWS Config API 작업을 사용한 태그 관리 ... 542
AWS 구성 규칙 ... 544
고려 사항 ... 544
리전 지원 ... 547
규칙의 구성 요소 ... 554
AWS Config 규칙 작동 방식 ... 554
트리거 유형 ... 555
평가 모드 ... 556
규칙 메타데이터 ... 557
관리형 규칙 ... 559
관리형 규칙 목록 ... 559

평가 모드별 관리형 규칙 목록 1020
트리거 유형별 관리형 규칙 목록 1043
리전 가용성별 관리형 규칙 목록 1065
AWS CloudFormation 템플릿을 사용하여 관리형 규칙 생성 1619
사용자 지정 규칙 1621
사용자 지정 정책 규칙 1621
사용자 지정 Lambda 규칙 1621
AWS Config 사용자 지정 규칙의 형식 차이 1622
사용자 지정 정책 규칙 생성 1622
사용자 지정 Lambda 규칙 생성 1628
사용자 지정 Lambda 규칙을 사용하여 삭제된 리소스 관리 1650
서비스 연결 규칙 1651
조직 규칙 1652
고려 사항 1653
배포 1654
리전 지원 1654
규칙 추가 1657
콘솔 사용 1658
AWS SDKs 사용 1660
규칙 업데이트 1664
콘솔 사용 1664
AWS SDKs 사용 1665
규칙 삭제 1668
고려 사항 1668
콘솔 사용 1669
AWS SDKs 사용 1670
규칙 확인 1671
콘솔 사용 1671
AWS SDKs 사용 1672
사전 평가 활성화 1681
콘솔 사용 1682
AWS SDKs 사용 1684
평가를 Security Hub로 전송 1688
규칙 평가를 Security Hub로 전송 1688
규칙을 사용하여 리소스 평가 1689
평가 결과 삭제 1693

문제 해결 ... 1694
적합성 팩 ... 1696
적합성 팩 대시보드 ... 1696
적합성 팩 기본 페이지 탐색 ... 1697
사전 조건 ... 1697
1단계: AWS Config 레코딩 시작 ... 1698
2단계: 적합성 팩 유형별 추가 사전 조건 ... 1698
리전 지원 ... 1703
프로세스 검사 ... 1709
샘플 템플릿 ... 1710
프로세스 검사 생성 ... 1711
규정 준수 상태 변경 ... 1711
보기 및 편집 ... 1712
적합성 팩 샘플 템플릿 ... 1713
AWS Control Tower Detective Guardrails 적합성 팩 ... 1717
ABS CCIG 2.0 중요 워크로드 운영 모범 사례 ... 1717
ABS CCIG 2.0 표준 워크로드 운영 모범 사례 ... 1900
ACSC Essential 8 운영 모범 사례 ... 2031
ACSC ISM 운영 모범 사례 ... 2050
AI 및 ML 운영 모범 사례 ... 2157
Amazon API Gateway 운영 모범 사례 ... 2157
Amazon CloudWatch 운영 모범 사례 ... 2158
Amazon DynamoDB 운영 모범 사례 ... 2158
Amazon S3 운영 모범 사례 ... 2158
APRA CPG 234 운영 모범 사례 ... 2158
자산 관리 운영 모범 사례 ... 2348
AWS Backup운영 모범 사례 ... 2348
AWS 자격 증명 및 액세스 관리를 위한 운영 모범 사례 ... 2349
AWS Well-Architected Framework 신뢰성 원칙의 운영 모범 사례 ... 2349
AWS Well-Architected Framework 보안 원칙의 운영 모범 사례 ... 2403
BCP 및 DR 운영 모범 사례 ... 2536
BNM RMiT 운영 모범 사례 ... 2536
캐나다 사이버 보안 센터(CCCS) 중간 클라우드 제어 프로필 운영 모범 사례 ... 2750
CIS AWS 파운데이션 벤치마크 v1.4 레벨 1 운영 모범 사례 ... 3970
CIS AWS 파운데이션 벤치마크 v1.4 레벨 2 운영 모범 사례 ... 4002
CIS Critical Security Controls v8 IG1 운영 모범 사례 ... 4043

CIS 핵심 보안 제어 v8 IG2 운영 모범 사례 4116
CIS 핵심 보안 제어 v8 IG3 운영 모범 사례 4249
CIS 운영 모범 사례 상위 20개 4393
CISA Cyber Essentials의 운영 모범 사례 4461
미국 연방수사국 형사사법정보부(CJIS) 운영 모범 사례 4612
CMMC 2.0 레벨 1 운영 모범 사례 4717
CMMC 2.0 레벨 2 운영 모범 사례 4814
컴퓨팅 서비스 운영 모범 사례 5137
데이터 복원력 운영 모범 사례 5137
데이터베이스 서비스 운영 모범 사례 5138
데이터 레이크 및 분석 서비스 운영 모범 사례 5138
DevOps 운영 모범 사례 5138
EC2 운영 모범 사례 5138
암호화 및 키 관리 운영 모범 사례 5138
SME를 위한 ENISA 사이버 보안 가이드 운영 모범 사례 5139
Esquema Nacional de Seguridad(ENS) Low 운영 모범 사례 5260
Esquema Nacional de Seguridad(ENS) Medium 운영 모범 사례 5353
Esquema Nacional de Seguridad(ENS) High 운영 모범 사례 5458
FDA 타이틀 21 CFR 파트 11 운영 모범 사례 5571
FedRAMP(Low) 운영 모범 사례 5823
FedRAMP(Moderate) 운영 모범 사례 6030
FedRAMP(High 파트 1) 운영 모범 사례 6456
FedRAMP(High 파트 2) 운영 모범 사례 6914
FFIEC 운영 모범 사례 7012
독일 C5(Cloud Computing Compliance Criteria Catalog) 운영 모범 사례 7183
Gramm Leach Bliley 법(GLBA) 운영 모범 사례 7252
GxP EU Annex 11 운영 모범 사례 7291
HIPAA 보안 운영 모범 사례 7410
IRS 1075 운영 모범 사례 7763
K-ISMS 운영 모범 사례 7909
로드 밸런싱 운영 모범 사례 7976
로깅 운영 모범 사례 7977
관리 및 거버넌스 서비스 운영 모범 사례 7977
MAS Notice 655 운영 모범 사례 7977
MAS TRMG 운영 모범 사례 8011
모니터링 운영 모범 사례 8194

NBC TRMG 운영 모범 사례 8195
NERC CIP BCSI 운영 모범 사례 8570
NCSC 클라우드 보안 원칙 운영 모범 사례 8616
NCSC 사이버 평가 프레임워크 운영 모범 사례 8701
네트워킹 및 콘텐츠 전송 서비스 운영 모범 사례 8843
NIST 800-53 rev 4 운영 모범 사례 8843
NIST 800-53 rev 5 운영 모범 사례 9103
NIST 800 171 운영 모범 사례 9628
NIST 800 172 운영 모범 사례 9905
NIST 800 181 운영 모범 사례 9964
NIST 1800 25 운영 모범 사례 10363
NIST CSF 운영 모범 사례 10494
NIST 개인정보보호 프레임워크 v1.0 운영 모범 사례 10779
NYDFS 23 운영 모범 사례 10975
NZISM 3.8 운영 모범 사례 11120
PCI DSS 3.2.1 운영 모범 사례 11233
PCI DSS 4.0 운영 모범 사례(글로벌 리소스 유형 제외) 11490
PCI DSS 4.0 운영 모범 사례(글로벌 리소스 유형 포함) 11744
공개적으로 액세스 가능한 리소스 운영 모범 사례 12060
UCB용 RBI 사이버 보안 프레임워크 운영 모범 사례 12060
RBI MD-ITF 운영 모범 사례 12102
보안, 자격 증명 및 규정 준수 서비스 운영 모범 사례 12216
서버리스 운영 모범 사례 12216
스토리지 서비스 운영 모범 사례 12216
SWIFT CSP 운영 모범 사례 12216
Amazon Elastic Container Service(Amazon ECS) 보안 모범 사례 12244
Amazon Elastic File System(Amazon EFS) 보안 모범 사례 12245
Amazon Elastic Kubernetes Service(Amazon EKS) 보안 모범 사례 12245
Amazon CloudFront 보안 모범 사례 12245
Amazon OpenSearch Service 보안 모범 사례 12245
Amazon Redshift 보안 모범 사례 12246
Amazon Relational Database Service(RDS) 보안 모범 사례 12246
AWS Auto Scaling보안 모범 사례 12246
AWS CloudTrail보안 모범 사례 12246
AWS CodeBuild보안 모범 사례 12246
Amazon ECR 보안 모범 사례 12247

AWS Lambda보안 모범 사례 12247
AWS Network Firewall보안 모범 사례 12247
Amazon SageMaker AI의 보안 모범 사례 12247
AWS Secrets Manager보안 모범 사례 12248
AWS WAF보안 모범 사례 12248
문제 해결 작업이 포함된 템플릿의 예 12248
사용자 지정 템플릿 생성 12248
용어 12249
템플릿 사용자 지정 12249
적합성 팩 배포 12253
적합성 팩 편집 12256
적합성 팩 삭제 12257
고려 사항 12258
적합성 팩을 삭제하려면 12258
적합성 팩 보기 12259
규정 준수 이력 보기 12262
규정 준수 타임라인 보기 12263
규정 준수 이력 쿼리 12263
조직 적합성 팩 관리 12265
고려 사항 12265
배포 12266
리전 지원 12267
문제 해결 12270
적합성 팩의 실패 상태 12270
적합성 팩의 누락 규칙 12271
문제 해결 12274
리전 지원 12274
수동 해결 작업 설정 12277
자동 해결 작업 설정 12279
해결 작업 삭제 12281
집계자 12283
사용 사례 12283
용어 12284
리전 지원 12284
애그리게이터 대시보드 12288
애그리게이터 대시보드 사용 12288

규정 준수 대시보드 12291
인벤토리 대시보드 12293
애그리게이터 생성 12295
위임된 관리자 등록 12300
애그리게이터 편집 12302
애그리게이터 삭제 12304
애그리게이터 계정 권한 부여 12305
고려 사항 12305
권한 부여 추가 12305
권한 부여 삭제 12307
고려 사항 12307
권한 부여 삭제 12308
애그리게이터 보기 12308
문제 해결 12310
고급 쿼리 12312
Features 12312
쿼리 구성 요소 12313
시놉시스 12313
파라미터 12313
예시 12314
쿼리 편집기(콘솔) 12314
고려 사항 12314
AWS 샘플 쿼리 사용 12315
사용자 정의 쿼리 생성 12315
쿼리 편집기(AWS CLI) 12316
고려 사항 12316
리소스 구성 데이터 쿼리 12317
쿼리를 저장합니다. 12319
저장된 모든 쿼리 보기 12319
저장된 쿼리의 세부 정보 조회 12320
저장된 쿼리 삭제 12320
자연어 쿼리 프로세서 12321
고려 사항 12321
자연어 쿼리 프로세서를 사용한 쿼리 12315
프롬프트 예제 12322
피드백 제공 12326

리전 지원 12326
쿼리 예제 12327
예제 관계 쿼리 12333
제한 사항 12334
CIDR 표기법/IP 범위 12336
배열 내의 여러 속성 12337
리전 지원 12337
데이터 삭제 12342
데이터 보존 기간 설정(콘솔) 12344
보안 12345
데이터 보호 12345
전송 중인 데이터 암호화 12346
전송 중인 데이터 암호화 12347
ID 및 액세스 관리 12347
대상 12347
ID를 통한 인증 12348
정책을 사용하여 액세스 관리 12351
AWS Config 에서 IAM을 사용하는 방법 12353
자격 증명 기반 정책 예제 12359
AWS 관리형 정책 12377
IAM 역할의 권한 12536
IAM 역할 업데이트 12541
Amazon S3 버킷에 대한 권한 12542
KMS 키에 대한 권한 12546
Amazon SNS 주제에 대한 권한 12548
문제 해결 12552
서비스 연결 역할 사용 12553
인시던트 대응 12555
규정 준수 검증 12556
복원성 12557
인프라 보안 12557
구성 및 취약성 분석 12558
교차 서비스 혼동된 대리자 방지 12558
모범 사례 12558
로깅 및 모니터링 12560
로깅 12560

AWS Config CloudTrail의 정보 12560
AWS Config 로그 파일 항목 이해 12561
로그 파일의 예 12561
모니터링 12569
Amazon SQS 사용 12569
Amazon EventBridge 사용 12572
Amazon VPC 엔드포인트 12578
VPC 엔드포인트 생성 12578
FAQ 12579
최신 구성 변경 사항을 볼 수 없습니다. 12579
구성 변경 사항을 즉시 볼 수 있나요? 12579
의 간접 관계 AWS Config 12579
리소스 관계란 무엇인가요? 12579
리소스에 대한 직접 관계와 간접 관계는 무엇인가요? 12580
가 AWS Config 지원하는 간접 관계는 무엇입니까? 12580
간접 관계를 사용하는 시나리오는 무엇입니까? 12582
직접 및 간접 관계로 인해 구성 항목이 어떻게 생성되나요? 12583
간접 관계로 인해 생성되는 구성 항목은 무엇인가요? 12583
간접 관계를 비활성화하려면 어떻게 해야 합니까? 12585
간접 관계와 관련된 구성 데이터를 검색하려면 어떻게 해야 하나요? 12586
코드 예제 12587
기본 사항 12587
작업 12588
문서 기록 12617
이전 업데이트 12744
..... 12804

란 무엇입니까 AWS Config?

AWS Config 는 계정 AWS 의 AWS 리소스 구성에 대한 자세한 보기를 제공합니다. 이러한 보기에는 리소스 간에 어떤 관계가 있는지와 리소스가 과거에 어떻게 구성되었는지도 포함되므로, 시간이 지나면서 구성과 관계가 어떻게 변하는지 확인할 수 있습니다.

An AWS resource는 Amazon Elastic Compute Cloud(EC2) 인스턴스 AWS, Amazon Elastic Block Store(EBS) 볼륨, 보안 그룹 또는 Amazon Virtual Private Cloud(VPC)와 같이 작업할 수 있는 엔터티입니다. 에서 지원하는 AWS 리소스의 전체 목록은 섹션을 AWS Config참조하세요에 대해 지원되는 리소스 유형 AWS Config.

고려 사항

- AWS 계정: 활성가 필요합니다 AWS 계정. 자세한 내용은 AWS등록을 참조하세요.
- Amazon S3 버킷: 구성 스냅샷 및 기록에 대한 데이터를 수신하려면 S3 버킷이 필요합니다. 자세한 내용을 알아보려면 Amazon S3 버킷에 대한 권한을 참조하세요.
- Amazon SNS 주제: 구성 스냅샷 및 기록 변경에 대한 알림을 받으려면 Amazon SNS가 필요합니다. 자세한 내용은 Amazon SNS 주제에 대한 권한을 참조하세요.
- IAM 역할: AWS Config에 액세스하는 데 필요한 권한이 있는 IAM 역할이 필요합니다. 자세한 내용은 IAM 역할 권한을 참조하세요.
- 리소스 유형: 기록할 리소스 유형을 결정할 수 AWS Config 있습니다. 자세한 내용은 AWS 리소스 레코딩을 참조하세요.

사용 방법 AWS Config

에서 애플리케이션을 실행할 때 AWS일반적으로 AWS 리소스를 사용하며, 리소스를 함께 생성하고 관리해야 합니다. 애플리케이션에 대한 수요가 계속 증가함에 따라 AWS 리소스를 추적해야 할 필요성도 증가합니다. AWS Config 는 다음 시나리오에서 애플리케이션 리소스를 감독하는 데 도움이 되도록 설계되었습니다.

리소스 관리

리소스 구성을 보다 효과적으로 관리하고 리소스 구성 오류를 발견하려면, 존재하는 리소스 및 이러한 리소스의 구성 방식을 언제든 세부적으로 파악할 수 있어야 합니다. AWS Config 를 사용하면 각 리소스에 대한 호출을 폴링하여 이러한 변경 사항을 모니터링할 필요 없이 리소스가 생성, 수정 또는 삭제될 때마다 알림을 받을 수 있습니다.

AWS Config 규칙을 사용하여 리소스의 구성 설정을 평가할 수 있습니다 AWS . 가 리소스가 규칙 중 하나의 조건을 위반하는 것을 AWS Config 감지하면는 리소스를 규정 미준수로 AWS Config 표시하고 알림을 보냅니다. AWS Config 는 리소스가 생성, 변경 또는 삭제될 때 리소스를 지속적으로 평가합니다.

감사, 보안 및 규정 준수

내부 정책 및 모범 사례를 준수하는지 확인하기 위해 감사가 자주 필요한 데이터를 작업할 수 있습니다. 보안 및 규정 준수를 입증하려면 리소스의 기록 구성에 액세스해야 합니다. 이 정보는에서 제공합니다 AWS Config.

구성 변경 관리 및 문제 해결

서로 의존하는 여러 AWS 리소스를 사용하는 경우 한 리소스의 구성이 변경되면 관련 리소스에 의도하지 않은 결과가 발생할 수 있습니다. 를 사용하면 수정하려는 리소스가 다른 리소스와 어떤 관련이 있는지 확인하고 변경의 영향을 평가할 AWS Config수 있습니다.

또한 AWS Config 에서 제공하는 리소스의 기록 구성을 사용하여 문제를 해결하고, 문제 리소스의 마지막으로 성공한 구성을 평가할 수 있습니다.

보안 분석

잠재적 보안 약점을 분석하려면 사용자에게 부여된 AWS Identity and Access Management (IAM) 권한 또는 AWS 리소스에 대한 액세스를 제어하는 Amazon EC2 보안 그룹 규칙과 같은 리소스 구성에 대한 자세한 기록 정보가 필요합니다.

AWS Config 를 사용하여가 기록 중인 언제든지 사용자, 그룹 또는 역할에 할당된 IAM 정책을 볼 수 AWS Config 있습니다. 이 정보를 통해 특정 시간에 사용자에 속한 권한을 확인할 수 있습니다. 예를 들어, 사용자 John Doe에게 2015년 1월 1일에 Amazon VPC 설정을 수정할 권한이 있었는지 여부를 볼 수 있습니다.

AWS Config 를 사용하여 특정 시간에 열린 포트 규칙을 포함하여 EC2 보안 그룹의 구성을 볼 수도 있습니다. 이 정보를 통해 보안 그룹이 특정 포트로 들어오는 TCP 트래픽을 차단했는지 여부를 확인할 수 있습니다.

파트너 솔루션

AWS 는 로깅 및 분석 분야의 타사 전문가와 협력하여 AWS Config 출력을 사용하는 솔루션을 제공합니다. 자세한 내용은의 AWS Config 세부 정보 페이지를 참조하세요AWS Config.

Features

설정 시 다음을 완료할 AWS Config수 있습니다.

리소스 관리

- AWS Config 기록할 리소스 유형을 지정합니다.

- 요청 시 구성 스냅샷 및 구성 기록을 수신하도록 Amazon S3 버킷을 설정합니다.
- 구성 스트림 알림을 보내도록 Amazon SNS 설정
- Amazon S3 버킷 및 Amazon SNS 주제에 액세스하는 데 필요한 AWS Config 권한을 부여합니다.

  자세한 내용은 AWS 리소스 구성 및 기록 보기 및 AWS 리소스 구성 및 기록 관리를 참조하세요.

규칙 및 적합성 팩

- 기록된 리소스 유형에 대한 규정 준수 정보를 평가하는 데 AWS Config 사용할 규칙을 지정합니다.
- 적합성 팩과 AWS 계정에서 단일 엔티티로 배포하고 모니터링할 수 있는 규칙 모음을 사용할 수 있습니다.

  자세한 내용은 AWS Config 규칙 및 적합성 팩을 사용하여 리소스 평가를 참조하세요.

문제 해결

- 에서 평가하는 규정 미준수 리소스를 수정합니다 AWS Config 규칙.

  자세한 정보는 해결 작업을 참조하세요.

집계자

- 집계자를 사용하면 리소스 인벤토리 및 규정 준수를 중앙에서 확인할 수 있습니다. 애그리게이터는 여러 AWS 계정 및 AWS 리전의 AWS Config 구성 및 규정 준수 데이터를 단일 계정 및 리전으로 수집합니다.

  자세한 내용은 다중 계정 다중 리전 데이터 집계를 참조하세요.

고급 쿼리

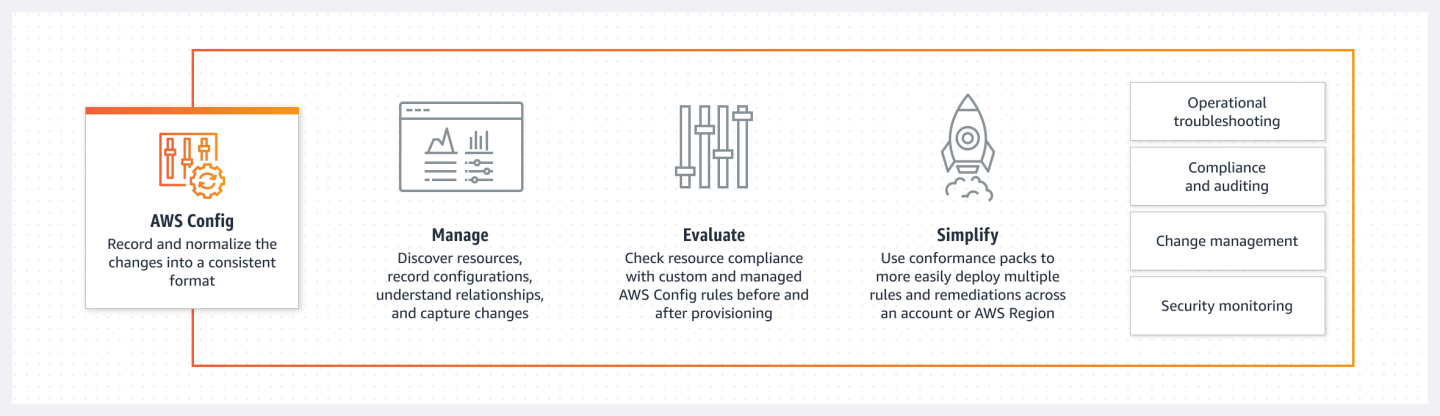
- AWS 리소스의 구성 스키마를 참조하여 샘플 쿼리 중 하나를 사용하거나 자체 쿼리를 작성합니다.

  자세한 내용은 AWS 리소스의 현재 구성 상태 쿼리를 참조하세요.

AWS Config 작동 방식

AWS Config 는 계정 AWS 의 AWS 리소스 구성에 대한 자세한 보기를 제공합니다. 이러한 보기에는 리소스 간에 어떤 관계가 있는지와 리소스가 과거에 어떻게 구성되었는지도 포함되므로, 시간이 지나면서 구성과 관계가 어떻게 변하는지 확인할 수 있습니다.

An AWS resource는 Amazon Elastic Compute Cloud(EC2) 인스턴스 AWS, Amazon Elastic Block Store(EBS) 볼륨, 보안 그룹 또는 Amazon Virtual Private Cloud(VPC)와 같이 작업할 수 있는 엔터티입니다. 에서 지원하는 AWS 리소스의 전체 목록은 섹션을 AWS Config참조하세요에 대해 지원되는 리소스 유형 AWS Config.



리소스 검색

켜면 AWS Config먼저 계정에 있는 지원되는 AWS 리소스를 검색하고 각 리소스에 대한 구성 항목을 생성합니다.

AWS Config 또한는 리소스의 구성이 변경될 때 구성 항목을 생성하고 구성 레코더를 시작한 시점부터 리소스의 구성 항목에 대한 기록 레코드를 유지합니다. 기본적으로는 리전에서 지원되는 모든 리소스에 대한 구성 항목을 AWS Config 생성합니다. 지원되는 모든 리소스 AWS Config 에 대한 구성 항목을 생성하지 않으려면 추적하려는 리소스 유형을 지정할 수 있습니다.

추적할 리소스 유형을 지정 AWS Config 하기 전에 리전 가용성별 리소스 적용 범위를 확인하여 리소스 유형이 설정 중인 AWS 리전에서 지원되는지 확인합니다 AWS Config. 리소스 유형이 하나 이상의 리전 AWS Config 에서에서 지원되는 경우 AWS Config지정된 리소스 유형이 설정 중인 리전에서 지

원되지 않더라도에서 지원하는 모든 AWS 리전에서 해당 리소스 유형의 기록을 활성화할 수 있습니다 AWS Config.

리소스 추적

AWS Config 는 계정의 각 리소스에 대해 설명 또는 목록 API 호출을 호출하여 리소스의 모든 변경 사항을 추적합니다. 이 서비스는 동일한 API 호출을 사용하여 모든 관련 리소스의 구성 세부 정보를 캡처합니다.

예를 들어 VPC 보안 그룹에서 송신 규칙을 제거 AWS Config 하면가 보안 그룹에서 Describe API 호출을 호출합니다. AWS Config 그런 다음는 보안 그룹과 연결된 모든 인스턴스에서 Describe API 호출을 호출합니다. 보안 그룹(리소스) 및 각 인스턴스(관련 리소스)의 업데이트된 구성은 구성 항목으로 기록되어 Amazon Simple Storage Service(S3) 버킷에 구성 스트림으로 전달됩니다.

AWS Config 또한는 API에서 시작하지 않은 구성 변경을 추적합니다.는 리소스 구성을 주기적으로 AWS Config 검사하고 변경된 구성에 대한 구성 항목을 생성합니다.

AWS Config 규칙을 사용하는 경우는 AWS 리소스 구성에서 원하는 설정을 AWS Config 지속적으로 평가합니다. 규칙에 따라 AWS Config 는 구성 변경에 대한 응답으로 또는 주기적으로 리소스를 평가합니다. 각 규칙은 이 규칙에 대한 평가 논리가 포함된 AWS Lambda 함수와 연결되어 있습니다. 가 리소스를 AWS Config 평가할 때 규칙의 AWS Lambda 함수를 호출합니다. 이 함수는 평가된 리소스의 준수 상태를 반환합니다. 리소스가 규칙의 조건을 위반하는 경우는 리소스와 규칙을 규정 미준수로 AWS Config 표시합니다. 리소스의 규정 준수 상태가 변경되면가 Amazon SNS 주제에 알림을 AWS Config 보냅니다.

구성 항목 전송

AWS Config 는 다음 채널 중 하나를 통해 구성 항목을 전달할 수 있습니다.

Amazon S3 버킷

AWS Config 는 AWS 리소스 구성의 변경 사항을 추적하고, 사용자가 지정한 Amazon S3 버킷에 업데이트된 구성 세부 정보를 정기적으로 전송합니다. 가 AWS Config 기록하는 각 리소스 유형에 대해 6시간마다 구성 기록 파일을 전송합니다. 각 구성 기록 파일에는 6시간 동안 변경된 리소스에 대한 세부 정보가 포함되어 있습니다. 각 파일에는 한 가지 유형의 리소스(예: Amazon EC2 인스턴스 또는 Amazon EBS 볼륨)가 포함되어 있습니다. 구성 변경이 발생하지 않으면 AWS Config 는 파일을 보내지 않습니다.

AWS Config AWS CLI에서 deliver-config-snapshot 명령을 사용하거나 AWS Config API에서 DeliverConfigSnapshot 작업을 사용할 때는 구성 스냅샷을 Amazon S3 버킷으로 전송합니다. 구성 스

냅샷에는 AWS Config 가 AWS 계정에 기록한 모든 리소스에 대한 구성 세부 정보가 포함되어 있습니다. 구성 기록 파일과 구성 스냅샷은 JSON 형식입니다.

> **Note**
>
> AWS Config 는 구성 기록 파일 및 구성 스냅샷만 지정된 S3 버킷으로 전송합니다. AWS Config 는 S3 버킷의 객체에 대한 수명 주기 정책을 수정하지 않습니다. 수명 주기 정책을 사용하여 객체를 삭제할지 Amazon S3 Glacier에 보관할지 지정할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 수명 주기 구성 관리를 참조하세요. 또한 S3 Glacier에 Amazon S3 데이터 보관 블로그 게시물을 참조하세요.

Amazon SNS 주제

Amazon Simple Notification Service(SNS) 주제는 Amazon SNS가 이메일 주소 또는 클라이언트와 같은 구독 엔드포인트에 메시지(또는 알림)를 전송하는 데 사용하는 커뮤니케이션 채널입니다. 다른 유형의 Amazon SNS 알림에는 휴대폰 앱에 전송되는 푸시 알림 메시지, SMS 수신 가능한 휴대폰 및 스마트폰에 전송되는 SMS(문자 서비스) 알림, HTTP POST 요청 등이 있습니다. 최상의 결과를 얻으려면 Amazon SQS를 SNS 주제의 알림 엔드포인트로 사용한 다음 알림의 정보를 프로그래밍 방식으로 처리합니다.

AWS Config 는 지정한 Amazon SNS 주제를 사용하여 알림을 보냅니다. 수신하는 알림 유형은 다음 예와 같이 메시지 본문에서 `messageType` 키의 값으로 표시됩니다.

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

알림은 다음 메시지 유형일 수 있습니다.

메시지 유형	설명
ComplianceChangeNotification	가 AWS Config 평가하는 리소스의 규정 준수 유형이 변경되었습니다. 규정 준수 유형은 리소스가 특정 AWS Config 규칙을 준수하는지 여부를 나타내며 메시지의 `ComplianceType` 키로 표시됩니다. 이 메시지에는 비교를 위해 `newEvaluationResult` 및 `oldEvaluationResult` 객체가 포함되어 있습니다.

메시지 유형	설명
ConfigRulesEvaluationStarted	AWS Config 가 지정된 리소스에 대해 규칙 평가를 시작했습니다.
ConfigurationSnapshotDeliveryStarted	AWS Config 가 구성 스냅샷을 Amazon S3 버킷으로 전송하기 시작했습니다. Amazon S3 버킷의 이름은 메시지에서 `s3Bucket` 키에 제공됩니다.
ConfigurationSnapshotDeliveryCompleted	AWS Config 가 구성 스냅샷을 Amazon S3 버킷에 성공적으로 전송했습니다.
ConfigurationSnapshotDeliveryFailed	AWS Config 가 Amazon S3 버킷으로 구성 스냅샷을 전송하지 못했습니다.
ConfigurationHistoryDeliveryCompleted	AWS Config 가 Amazon S3 버킷에 구성 기록을 성공적으로 전송했습니다.
ConfigurationItemChangeNotification	리소스가 구성에서 생성, 삭제 또는 변경되었습니다. 이 메시지에는이 변경에 대해가 AWS Config 생성하는 구성 항목의 세부 정보와 변경 유형이 포함됩니다. 이러한 알림은 변경 후 몇 분 이내에 전달되며, 구성 스트림이라고 통칭합니다.
OversizedConfigurationItemChangeNotification	구성 항목 변경 알림이 Amazon SNS에서 허용하는 최대 크기를 초과한 경우 이 메시지 유형이 전달됩니다. 이 메시지에는 구성 항목의 요약이 포함됩니다. SMS 메시지를 제외한 Amazon SNS 메시지는 XML, JSON 및 형식이 지정되지 않은 텍스트를 포함하여 최대 256KB의 텍스트 데이터를 포함할 수 있습니다. 지정한 Amazon S3 버킷 위치에서 완료 알림을 볼 수 있습니다.
OversizedConfigurationItemChangeDeliveryFailed	AWS Config 가 Amazon S3 버킷에 크기 초과 구성 항목 변경 알림을 전달하지 못했습니다.

알림 예는 가 Amazon SNS 주제로 AWS Config 보내는 알림 문서를 참조하세요. Amazon SNS에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 안내서를 참조하세요.

> **Note**
>
> 최신 구성 변경 사항을 볼 수 없습니다.
> AWS Config 는 일반적으로 변경 사항이 감지된 직후 또는 지정한 빈도로 리소스에 대한 구성 변경 사항을 기록합니다. 그러나 이는 가장 이상적인 시나리오이며 경우에 따라 더 오래 걸릴 수 있습니다. 문제가 일정 시간 후에도 지속되면 지원에 문의하여 Amazon CloudWatch에서 지원하는 AWS Config 지표를 제공하세요. 이러한 지표에 대한 자세한 내용은 AWS Config 사용량 및 성공 지표를 참조하세요.

에 대한 액세스 제어 AWS Config

AWS Identity and Access Management 는 Amazon Web Services(AWS) 고객이 사용자 및 사용자 권한을 관리할 수 있는 웹 서비스입니다.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요:

- 의 사용자 및 그룹 AWS IAM Identity Center:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따릅니다.
- 보안 인증 공급자를 통해 IAM에서 관리되는 사용자:

  ID 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 Create a role for a third-party identity provider (federation)의 지침을 따릅니다.
- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 Create a role for an IAM user의 지침을 따릅니다.
  - (권장되지 않음)정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따르세요.

AWS Config 용어 및 개념

이해를 돕기 위해 AWS Config이 주제에서는 몇 가지 주요 개념을 설명합니다.

목차

- AWS Config 인터페이스
  - AWS Config 콘솔
  - AWS Config CLI
  - AWS Config APIs
  - AWS Config SDKs
- 리소스 관리
  - AWS 리소스
  - 리소스 관계
- 구성 레코더
- 전송 채널
  - 구성 항목
  - 구성 기록
  - 구성 스냅샷
  - 구성 스트림
- AWS Config 규칙
  - 평가 결과
  - 규칙 유형
  - 트리거 유형
  - 평가 모드
- 적합성 팩
- 다중 계정 다중 리전 데이터 집계
  - 소스 계정
  - 소스 리전
  - 집계자
  - 서비스 연결 집계자
  - 집계자 계정
  - 권한 부여

AWS Config 인터페이스

AWS Config 콘솔

AWS Config 콘솔을 사용하여 서비스를 관리할 수 있습니다. 에 대한 자세한 내용은 섹션을 AWS Management Console참조하세요AWS Management Console.

AWS Config CLI

AWS Command Line Interface 는 명령줄 AWS Config 에서 상호 작용하는 데 사용할 수 있는 통합 도구입니다. 자세한 내용은 AWS Command Line Interface 사용 설명서를 참조하십시오. AWS Config CLI 명령의 전체 목록은 사용 가능한 명령을 참조하세요.

AWS Config APIs

콘솔 및 CLI 외에도 AWS Config RESTful APIs를 사용하여 AWS Config 직접 프로그래밍할 수도 있습니다. 자세한 내용은 AWS Config API 참조를 참조하세요.

AWS Config SDKs

AWS Config API를 사용하는 대신 AWS SDKs. 각 SDK는 다양한 프로그래밍 언어 및 플랫폼을 위한 라이브러리와 샘플 코드로 구성되어 있습니다. SDK를 사용하면 편리하게 AWS Config에 프로그래밍 방식으로 액세스할 수 있습니다. 예를 들어, SDK를 사용하여 요청에 암호화 방식으로 서명하고, 오류를 관리하며, 자동으로 요청을 재시도할 수 있습니다. 자세한 내용은 Amazon Web Services의 도구 페이지를 참조하세요.

리소스 관리

의 기본 구성 요소를 이해 AWS Config 하면 리소스 인벤토리 및 변경 사항을 추적하고 AWS 리소스 구성을 평가하는 데 도움이 됩니다.

AWS 리소스

AWS 리소스는 AWS Management Console, AWS Command Line Interface (CLI), AWS SDKs. AWS 리소스의 AWS 예로는 Amazon EC2 인스턴스, 보안 그룹, Amazon VPCs 및 Amazon Elastic Block Store가 있습니다.는 리소스 ID 또는 Amazon 리소스 이름(ARN)과 같은 고유 식별자를 사용하여 각 리소스를 AWS Config 참조합니다. 에서 AWS Config 지원하는 리소스 유형 목록은 섹션을 참조하세요에 대해 지원되는 리소스 유형 AWS Config.

리소스 관계

AWS Config 는 계정에서 AWS 리소스를 검색한 다음 AWS 리소스 간의 관계 맵을 생성합니다. 예를 들어, 관계에는 보안 그룹 `sg-ef678hk`과 관련된 Amazon EC2 인스턴스 `i-a1b2c3d4`에 연결된 Amazon EBS 볼륨 `vol-123ab45d`이 포함될 수 있습니다.

자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 섹션을 참조하세요.

구성 레코더

구성 레코더는 범위 내 리소스 유형에 대한 구성 변경 사항을 구성 항목으로 저장합니다. 자세한 내용은 구성 레코더 작업 단원을 참조하십시오.

구성 레코더에는 두 가지 유형이 있습니다.

유형	설명
고객 관리형 구성 레코더	관리한 구성 레코더입니다. 범위의 리소스 유형은 사용자가 설정합니다. 기본적으로 고객 관리형 구성 레코더는 AWS Config 이 실행되는 AWS 리전 에서 지원되는 모든 리소스를 기록합니다.
서비스 연결 구성 레코더	특정에 연결된 구성 레코더입니다 AWS 서비스. 범위의 리소스 유형은 연결된 서비스에 의해 설정됩니다.

전송 채널

는 AWS 리소스에 발생하는 변경 사항을 AWS Config 지속적으로 기록하므로 전송 채널을 통해 알림과 업데이트된 구성 상태를 전송합니다. 전송 채널을 관리하여가 구성 업데이트를 AWS Config 보내는 위치를 제어할 수 있습니다.

구성 항목

구성 항목은 계정에 있는 지원되는 AWS 리소스의 다양한 속성에 대한 point-in-time 보기를 나타냅니다. 구성 항목의 구성 요소에는 메타데이터, 속성, 관계, 현재 구성 및 관련 이벤트가 포함됩니다.는 기록 중인 리소스 유형에 대한 변경을 감지할 때마다 구성 항목을 AWS Config 생성합니다. 예를 들어 AWS Config 가 Amazon S3 버킷을 기록하는 경우는 버킷이 생성, 업데이트 또는 삭제될 때마다 구성

항목을 AWS Config 생성합니다. 에 대해 AWS Config 를 선택하여 설정한 레코딩 빈도로 구성 항목을 생성할 수도 있습니다.

자세한 내용은 Components of a Configuration Item 및 레코딩 빈도를 참조하세요.

구성 기록

구성 기록은 임의의 기간 동안 지정된 리소스에 대한 구성 항목의 모음입니다. 구성 기록을 통해 리소스가 처음 생성된 시간, 리소스가 지난 한 달간 구성된 방법, 어제 오전 9시에 도입된 구성 변경에 대한 질문에 답할 수 있습니다. 구성 기록은 여러 형식으로 사용할 수 있습니다.는 사용자가 지정한 Amazon S3 버킷에 기록되는 각 리소스 유형에 대한 구성 기록 파일을 AWS Config 자동으로 전송합니다. AWS Config 콘솔에서 지정된 리소스를 선택하고 타임라인을 사용하여 해당 리소스의 이전 구성 항목으로 모두 이동할 수 있습니다. 또한 API에서 리소스의 구성 기록 항목에 액세스할 수도 있습니다.

자세한 내용은 규정 준수 기록 보기 및 규정 준수 기록 쿼리를 참조하세요.

구성 스냅샷

구성 스냅샷은 계정에 있는 지원되는 리소스에 대한 구성 항목의 모음입니다. 이 구성 스냅샷은 기록 중인 리소스와 그 구성의 전체 사진입니다. 구성 스냅샷은 구성의 유효성을 검사할 때 유용한 도구일 수 있습니다. 예를 들어, 잘못 구성되었거나 없어야 하는 리소스의 구성 스냅샷을 정기적으로 검토하고자 할 수 있습니다. 구성 스냅샷은 여러 형식으로 제공됩니다. 구성 스냅샷이 지정한 Amazon Simple Storage Service(S3) 버킷으로 전달되도록 할 수 있습니다. 또한 AWS Config 콘솔에서 특정 시점을 선택하고 리소스 간의 관계를 사용하여 구성 항목의 스냅샷을 탐색할 수 있습니다.

자세한 내용은 구성 스냅샷 전송, 구성 스냅샷 보기 및 구성 스냅샷 예제를 참조하세요.

구성 스트림

구성 스트림은 기록 중인 리소스에 대한 모든 구성 항목의 자동 업데이트 목록 AWS Config 입니다. 리소스가 생성, 수정 또는 삭제될 때마다 AWS Config 는 구성 항목을 만들고 구성 스트림에 추가합니다. 구성 스트림은 선택한 Amazon Simple Notification Service(SNS) 주제를 사용하여 작동합니다. 구성 스트림은 구성 변경 사항이 발생할 때 이를 관찰하여 잠재적 문제를 발견하거나, 특정 리소스가 변경되면 알림을 생성하거나, AWS 리소스의 구성을 반영해야 하는 외부 시스템을 업데이트하는 데 유용합니다.

AWS Config 규칙

AWS Config 규칙은 특정 AWS 리소스에 대한 이상적인 구성 설정을 관리하는 데 도움이 되는 규정 준수 검사입니다.는 리소스 구성이 관련 규칙을 준수하는지 여부를 AWS Config 평가하고 규정 준수 결과를 표시합니다.

평가 결과

AWS Config 규칙에 대해 네 가지 평가 결과가 있을 수 있습니다.

평가 결과	설명
COMPLIANT	규칙은 규정 준수 검사 조건을 전달합니다.
NON_COMPLIANT	규칙이 규정 준수 검사 조건에 실패합니다.
ERROR	필수/선택 사항 파라미터 중 하나가 유효하지 않거나, 올바른 유형이 아니거나, 형식이 잘못되었습니다.
NOT_APPLICABLE	규칙의 로직을 적용할 수 없는 리소스를 필터링하는 데 사용됩니다. 예를 들어 alb-desync-mode-check 규칙은 Application Load Balancer만 검사하고 Network Load Balancer 및 Gateway Load Balancer는 무시합니다.

규칙 유형

두 가지 유형의 규칙이 있습니다. 규칙 정의 및 규칙 메타데이터의 구조에 대한 자세한 내용은 AWS Config 규칙의 구성 요소를 참조하세요.

유형	설명	추가 정보
관리형 규칙	에서 생성한 사전 정의되고 사용자 지정 가능한 규칙입니다 AWS Config.	관리형 규칙 목록은 AWS Config 관리형 규칙 목록을 참조하세요.
사용자 지정 규칙	처음부터 생성하는 규칙입니다. AWS Config 사용자 지정 규칙을 생성하는 방법에는 Lambda 함수(AWS Lambda 개발자 안내서)와 Guard(Guard GitHub 리포지토리)의 두 가지가 있습니다.	자세한 내용은 사용자 지정 정책 규칙 생성 AWS Config 및 AWS Config 사용자 지정 Lambda 규칙 생성을 참조하세요.

트리거 유형

계정에 규칙을 추가한 후는 리소스와 규칙 조건을 AWS Config 비교합니다. 이 초기 평가 후는 평가가 트리거될 때마다 평가를 AWS Config 계속 실행합니다. 평가 트리거는 규칙의 일부로 정의되어 있으며, 다음 유형을 포함할 수 있습니다.

트리거 유형	설명
구성 변경	AWS Config 는 규칙의 범위와 일치하는 리소스가 있고 리소스의 구성이 변경되면 규칙에 대한 평가를 실행합니다. 평가는가 구성 항목 변경 알림을 AWS Config 전송한 후 실행됩니다. 규칙의 범위를 정의하여 평가를 유발하는 리소스를 선택합니다. 범위에는 다음이 포함될 수 있습니다. • 하나 이상의 리소스 유형 • 리소스 유형과 리소스 ID의 조합 • 태그 키와 값의 조합 • 기록된 모든 리소스가 생성, 업데이트 또는 삭제된 때 AWS Config 는 규칙의 범위와 일치하는 리소스에 대한 변경을 감지하면 평가를 실행합니다. 범위를 사용하여 평가를 시작하는 리소스를 제한할 수 있습니다.
주기적	AWS Config 는 규칙 평가를 선택한 빈도로 실행합니다. 예를 들어 24시간마다 실행합니다.
하이브리드	일부 규칙에는 구성 변경과 주기적 트리거가 모두 있습니다. 이러한 규칙의 경우는 구성 변경을 감지할 때와 지정한 빈도로 리소스를 AWS Config 평가합니다.

평가 모드

AWS Config 규칙에 대한 두 가지 평가 모드가 있습니다.

평가 모드	설명
사전	리소스를 배포하기 전에 평가하려면 사전 평가를 사용합니다. 이렇게 하면 리소스 속성 집합을 사용하여 리소스를 정의하는 경우 해당 리전의 계정에 있는 사전 예방 규칙 집합을 고려하여 해당 AWS 리소스 속성 집합이 COMPLIANT인지 NON_COMPLIANT인지 평가할 수 있습니다. 자세한 내용은 평가 모드를 참조하세요. 사전 평가를 지원하는 관리형 규칙 목록은 평가 모드별 AWS Config 관리형 규칙 목록을 참조하세요.
탐지	탐지 평가를 통해 이미 배포된 리소스를 평가합니다. 이를 통해 기존 리소스의 구성 설정을 평가할 수 있습니다.

> **Note**
> 사전 예방 규칙은 NON_COMPLIANT로 플래그가 지정된 리소스를 수정하거나 배포를 금지하지 않습니다.

적합성 팩

적합성 팩은 계정 및 리전의 단일 엔터티로 또는의 조직 전체에 쉽게 배포할 수 있는 AWS Config 규칙 및 문제 해결 작업의 모음입니다 AWS Organizations.

적합성 팩은 AWS Config 관리형 규칙이나 사용자 지정 규칙 및 문제 해결 작업의 목록이 포함된 YAML 템플릿을 작성하여 만듭니다. AWS Config 콘솔 또는 AWS CLI를 사용하여 템플릿을 배포할 수 있습니다.

빠르게 시작하고 AWS 환경을 평가하려면 샘플 적합성 팩 템플릿 중 하나를 사용합니다. 또한 사용자 지정 적합성 팩을 기반으로 적합성 팩 YAML 파일을 처음부터 작성할 수도 있습니다. 사용자 지정 적합

성 팩은 계정과 AWS 리전 또는의 조직 전체에 함께 배포할 수 있는 고유한 AWS Config 규칙 및 문제 해결 작업 모음입니다 AWS Organizations.

프로세스 검사는 적합성 팩의 일부로 확인이 필요한 외부 및 내부 작업을 추적할 수 있는 AWS Config 규칙의 한 유형입니다. 이러한 검사를 기존 적합성 팩이나 새 적합성 팩에 추가할 수 있습니다. 한 위치에서 AWS Config요 및 수동 검사를 포함하는 모든 규정 준수를 추적할 수 있습니다.

다중 계정 다중 리전 데이터 집계

의 다중 계정 다중 리전 데이터 집계 AWS Config 를 사용하면 여러 계정 및 리전의 구성 및 규정 준수 데이터를 단일 계정으로 집계 AWS Config 할 수 있습니다. 다중 계정 다중 리전 데이터 집계는 중앙 IT 관리자가 엔터프라이즈 AWS 계정 의 여러에 대한 규정 준수를 모니터링하는 데 유용합니다. 애그리게이터를 사용해도 추가 비용이 발생하지 않습니다.

소스 계정

소스 계정은 AWS Config 리소스 구성 및 규정 준수 데이터를 집계하려는 AWS 계정 입니다. 소스 계정은 개별 계정일 수도 있고 AWS Organizations내 조직일 수도 있습니다. 소스 계정을 개별적으로 제공하거나 검색할 수 있습니다 AWS Organizations.

소스 리전

소스 리전은 AWS Config 구성 및 규정 준수 데이터를 집계하려는 AWS 리전입니다.

집계자

애그리게이터는 여러 소스 계정 및 리전에서 AWS Config 구성 및 규정 준수 데이터를 수집합니다. 집계된 AWS Config 구성 및 규정 준수 데이터를 보려는 리전에 집계자를 생성합니다.

> **Note**
>
> 애그리게이터는 소스 계정의 데이터를 애그리게이터 계정으로 복제하여 애그리게이터가 볼 권한을 부여받은 소스 계정 및 리전에 대한 읽기 전용 보기를 제공합니다. 애그리게이터는 소스 계정 또는 리전에 대한 변형 액세스 권한을 제공하지 않습니다. 예를 들어, 애그리게이터를 통해 규칙을 배포하거나, 애그리게이터를 통해 소스 계정 또는 리전으로 스냅샷 파일을 보낼 수 없습니다.

서비스 연결 집계자

서비스 연결 집계자는 특정에 연결됩니다 AWS 서비스. 범위 내 구성 및 규정 준수 데이터는 연결된 서비스에 의해 설정됩니다.

집계자 계정

애그리게이터 계정은 사용자가 애그리게이터를 생성하는 계정입니다.

권한 부여

소스 계정 소유자인 권한 부여는 AWS Config 구성 및 규정 준수 데이터를 수집하기 위해 애그리게이터 계정 및 리전에 부여하는 권한을 말합니다. AWS Organizations를 구성하는 소스 계정을 집계하는 경우에는 권한 부여가 필요하지 않습니다.

AWS 와의 서비스 통합 AWS Config

AWS Config 는 여러 다른 AWS 서비스와의 통합을 지원합니다. 이 목록은 일반 목록이 아닙니다.

AWS Organizations

AWS Organizations 를 사용하여 AWS Config의 다중 계정, 다중 리전 데이터 집계 기능에 사용할 계정을 정의할 수 있습니다. AWS Organizations 는 여러를 생성하여 중앙 AWS 계정 에서 관리하는 조직에 통합하는 데 도움이 되는 계정 관리 서비스입니다. AWS Organizations 세부 정보를 제공하여 조직 전반의 규정 준수 상태를 모니터링할 수 있습니다. 자세한 내용은 AWS Organizations 사용 설명서의 AWS Config , AWS Organizations 페이지를 참조하세요.

AWS Control Tower

AWS Control Tower 는 등록된 모든 계정 AWS Config 에서를 활성화하므로 탐지 제어를 통해 규정 준수를 모니터링하고, 리소스 변경을 기록하고, 리소스 변경 로그를 로그 아카이브 계정으로 전달할 수 있습니다. 자세한 내용은 AWS Control Tower 사용 설명서에서 AWS Config을 사용한 리소스 변경 모니터링을 참조하세요.

AWS CloudTrail

AWS Config 는와 통합되어 계정의 특정 이벤트와 구성 변경 간의 AWS CloudTrail 상관관계를 파악합니다. CloudTrail 로그를 사용하여 누가, 언제, 어떤 IP 주소에서 요청을 했는지를 포함하여 변경을 호출한 이벤트의 세부 정보를 얻을 수 있습니다. CloudTrail 콘솔에서 AWS Config 타임라인으로 이동하여 AWS API 활동과 관련된 구성 변경 사항을 볼 수 있습니다.

자세한 내용은 AWS Config 개발자 안내서의 를 사용하여 AWS Config API 호출 로깅 AWS CloudTrail 및 AWS CloudTrail 사용 설명서의 콘솔을 사용하여 AWS Config 구성 항목에 대한 이벤트 데이터 스토어 생성을 참조하세요.

AWS Security Hub

AWS Security Hub 는 AWS Config 규칙을 포함한 다른 AWS 서비스의 보안 검사를 중앙 집중화합니다. Security Hub는 AWS Config 규칙을 활성화하고 제어하여 리소스 구성이 모범 사례에 부합하는지 확인합니다. Security Hub가 환경의 리소스에 AWS Config 대한 보안 검사를 실행하는 모든 리전의 모든 계정에서를 활성화합니다. 자세한 내용은 AWS Security Hub 사용 설명서의 AWS Security Hub로 조사 결과를 보내는 서비스를 참조하세요.

> 일부 Security Hub 관련 규칙은 주기적이며 구성 항목에 의존하지 않습니다.
>
> 일부 Security Hub 관련 규칙은 주기적입니다. 이러한 규칙은 구성 레코더를 활성화하지 않고 실행할 수 있으며 구성 항목(CI)에 의존하지 않습니다.
> 즉, 규칙 페이지를 보면 나열된 CI 또는 지원되는 리소스가 없습니다. 리소스 ID를 선택하면 오류가 표시됩니다`The provided resource ID and resource type cannot be found`. 이는 예상된 동작입니다.

AWS Trusted Advisor

AWS Config 관리형 규칙은 모든 범주에서 Trusted Advisor 일련의 검사를 지원합니다. 특정 관리형 규칙을 활성화하면 해당 Trusted Advisor 검사가 자동으로 활성화됩니다. 특정 AWS Config 관리형 규칙으로 구동되는 Trusted Advisor 검사를 확인하려면 AWS Support 사용 설명서의 AWS Trusted Advisor 확인 참조를 참조하세요.

AWS Business Support, AWS Enterprise On-Ramp 및 AWS Enterprise Support 플랜을 보유한 고객은 AWS Config 파워 체크를 사용할 수 있습니다. 를 활성화 AWS Config 하고 이러한 AWS 지원 플랜 중 하나가 있는 경우 해당 배포된 AWS Config 관리형 규칙으로 구동되는 권장 사항이 자동으로 표시됩니다.

> 새로 고침 요청은 허용되지 않으며 리소스를 제외할 수 없습니다.
>
> 이러한 검사의 결과는 AWS Config 관리형 규칙에 대한 변경 트리거 업데이트를 기반으로 자동으로 새로 고쳐집니다. 새로 고침 요청은 허용되지 않습니다. 현재 이러한 검사에서 리소스를 제외할 수 없습니다.

자세한 내용은 AWS Support 사용 설명서의 에서 제공하는 Trusted Advisor 검사 보기를 AWS Config 참조하세요.

AWS Audit Manager

Audit Manager를 사용하여 AWS Config 평가를 감사의 증거로 캡처할 수 있습니다. 사용자 지정 컨트롤을 생성하거나 편집할 때 하나 이상의 AWS Config 규칙을 증거 수집을 위한 데이터 소스 매핑으로 지정할 수 있습니다.는 이러한 규칙을 기반으로 규정 준수 검사를 AWS Config 수행하고 Audit Manager는 결과를 규정 준수 확인 증거로 보고합니다. 자세한 내용은 AWS Audit Manager 사용 설명서의 AWS Audit Manager지원AWS Config 규칙을 참조하세요.

AWS Systems Manager

AWS Config 는 Systems Manager와 통합되어 온프레미스 환경의 Amazon EC2 인스턴스 및 서버의 소프트웨어에 대한 구성 변경을 기록합니다. 이 통합을 통해 운영 체제(OS) 구성, 시스템 수준 업데이트, 설치된 애플리케이션, 네트워크 구성 등에 대한 가시성을 확보할 수 있습니다. AWS Config 은 Amazon EC2 인스턴스에 대해 기록된 인프라 구성 변경 사항과 함께 OS 및 시스템 수준 구성 변경 사항의 기록을 제공할 수도 있습니다. Systems Manager 콘솔에서 AWS Config 타임라인으로 이동하여 관리형 Amazon EC2 인스턴스의 구성 변경 사항을 볼 수 있습니다. AWS Config 를 사용하여 Systems Manager 인벤토리 기록을 보고 모든 관리형 인스턴스의 변경 사항을 추적할 수 있습니다.

자세한 내용은 AWS Systems Manager 사용 설명서의 AWS 서비스 통합 | 관리 및 거버넌스, AWS Config 구성 레코더 및 AWS Config 적합성 팩 배포를 참조하세요.

AWS Firewall Manager

Firewall Manager를 사용하려면 각 AWS Organizations 멤버 계정에 AWS Config 대해를 활성화해야 합니다. 새 애플리케이션이 생성되면 Firewall Manager는 방화벽 규칙을 구축하고, 보안 정책을 생성하고, 일관되게 적용하는 단일 서비스 역할을 수행합니다. 자세한 내용은 AWS WAF AWS Firewall Manager, 및 AWS Shield Advanced 개발자 안내서의 활성화 AWS Config를 참조하세요.

> **Note**
>
> Firewall Manager는 리소스를 모니터링하기 위해 지속적인 기록에 의존합니다. Firewall Manager를 사용하는 경우 기록 빈도를 계속으로 설정하는 것이 좋습니다. 연속 기록 및 일일 기록에 대한 자세한 내용은 레코딩 빈도 페이지를 참조하세요.

Amazon EC2 전용 호스트

AWS Config 는 Amazon EC2 전용 호스트와 통합되어 라이선스 규정 준수를 평가합니다.는 전용 호스트에서 인스턴스가 시작, 중지 또는 종료될 때를 AWS Config 기록하고이 정보를 호스트 ID, Amazon Machine Image(AMI) IDs, 소켓 수, 물리적 코어와 같은 소프트웨어 라이선스와 관련된 호스트 및 인스턴스 수준 정보와 페어링합니다. 이를 통해를 라이선스 보고의 데이터 소스 AWS Config 로 사용할 수 있습니다. Amazon EC2 전용 호스트 콘솔에서 AWS Config 타임라인으로 이동하여 Amazon EC2 전용 호스트의 구성 변경 사항을 볼 수 있습니다.

자세한 내용은 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서의 구성 변경 사항 추적 또는 Windows 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서의 구성 변경 사항 추적을 참조하세요.

Application Load Balancers

AWS Config 는 Elastic Load Balancing(ELB) 서비스와 통합되어 Application Load Balancer에 대한 구성 변경을 기록합니다. 에는 연결된 Amazon EC2 보안 그룹, VPCs 및 서브넷과의 관계 AWS Config 도 포함됩니다. 이러한 정보는 보안 및 문제 해결에 활용할 수 있습니다. 예를 들어 언제든지 Application Load Balancer와 연결된 보안 그룹을 확인할 수 있습니다. ELB 콘솔에서 AWS Config 타임라인으로 이동하여 Application Load Balancer의 구성 변경 사항을 볼 수 있습니다.

AWS CodeBuild

AWS Config는 AWS 리소스 인벤토리와 이러한 리소스에 대한 구성 변경 기록을 제공합니다.는 AWS 리소스로 AWS CodeBuild를 AWS Config 지원합니다. 즉, 서비스가 CodeBuild 프로젝트를 추적할 수 있습니다. 자세한 내용은 AWS CodeBuild 사용 설명서의 CodeBuild 샘플과 AWS Config 함께 사용을 참조하세요.

AWS X-Ray

AWS X-Ray 는와 통합되어 X-Ray 암호화 리소스에 대한 구성 변경을 AWS Config 기록합니다. AWS Config 를 사용하여 X-Ray 암호화 리소스를 인벤토리하고, X-Ray 구성 기록을 감사하고, 리소스 변경 사항에 따라 알림을 보낼 수 있습니다. 자세한 내용은 AWS X-Ray 개발자 안내서의 AWS Config을 사용한 X-Ray 암호화 구성 변경 사항 추적을 참조하세요.

AWS Service Management Connector

AWS Service Management Connector for ServiceNow는 집계자를 사용하여 여러 계정 및 리전의 AWS Config 데이터를 동기화할 수 있습니다. 자세한 내용은 AWS Service Management Connector 관리자 안내서의 ServiceNow AWS Config 에서 통합을 참조하세요.

Amazon API Gateway

AWS Config 를 사용하여 API Gateway API 리소스에 대한 구성 변경을 기록하고 리소스 변경 사항에 따라 알림을 보낼 수 있습니다. API Gateway 리소스에 대한 구성 변경 기록을 유지 관리하면 운영 문제 해결, 감사 및 규정 준수 사용 사례에 도움이 됩니다. 자세한 내용은 API Gateway 개발자 안내서의 AWS Config을 사용한 API Gateway API 구성 모니터링을 참조하세요.

에 대한 리전 지원 AWS Config

고려 사항

의 일부 기능은 AWS Config 가 지원되는 AWS 리전의 하위 집합에서만 지원 AWS Config 됩니다.

리소스 관리

- 리전에서 지원되는 AWS 리소스 유형의 목록은 리전 가용성별 리소스 범위를 참조하세요.

AWS Config 규칙

- 리전에서 지원되는 AWS Config 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.
- AWS Config 규칙의 조직 배포를 지원하는 리전 목록은 조직 규칙 | 리전 지원을 참조하세요.

적합성 팩

- 적합성 팩 및 적합성 팩의 조직 배포를 지원하는 리전의 목록은 적합성 팩 | 리전 지원을 참조하세요.

문제 해결

- AWS Config 규칙에 대한 문제 해결 작업을 지원하는 리전 목록은 문제 해결 작업 | 리전 지원을 참조하세요.

집계자

- 집계자를 지원하는 리전의 목록은 집계자 | 리전 지원을 참조하세요.

고급 쿼리

- 고급 쿼리를 지원하는 리전의 목록은 고급 쿼리 | 리전 지원을 참조하세요.
- 고급 쿼리용 자연어 쿼리 프로세서를 지원하는 리전 목록은 고급 쿼리용 자연어 쿼리 프로세서 | 리전 지원을 참조하세요.

지원되는 리전 목록

다음 표에는 활성화할 수 있는 AWS 리전이 나열되어 있습니다 AWS Config.

리전 이름	지역	엔드포인트	프로토콜
미국 동부 (오하이오)	us-east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS
미국 동부 (버지니아 북부)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
미국 서부 (캘리포니아 북부)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
미국 서부 (오레곤)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
아프리카 (케이프타운)	af-south-1	config.af-south-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(홍콩)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
아시아 태평양(하이데라바드)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
아시아 태평양(자카르타)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
아시아 태평양(말레이시아)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
아시아 태평양(멜버른)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
아시아 태평양(뭄바이)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
아시아 태평양(오사카)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
아시아 태평양(서울)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(시드니)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
아시아 태평양(타이베이)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
아시아 태평양(태국)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
아시아 태평양(도쿄)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
캐나다(중부)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
캐나다 서부(캘거리)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
유럽(프랑크푸르트)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
유럽(아일랜드)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
유럽(런던)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
유럽(밀라노)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
유럽(파리)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
유럽(스페인)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
유럽(스톡홀름)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
유럽(취리히)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
이스라엘(텔아비브)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
멕시코(중부)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
중동(바레인)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
중동(UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
남아메리카(상파울루)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 동부)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 서부)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

에 대한 서비스 제한 AWS Config

다음 표에서는 내의 제한에 대해 설명합니다 AWS Config. 특별한 언급이 없는 한 요청 시 할당량을 높일 수 있습니다. 할당량 증가를 요청할 수 있습니다.

의 다른 제한에 대한 자세한 내용은 서비스 제한을 AWS참조하세요. AWS

리소스 태그

설명	제한 값	높일 수 있음
리소스당 최대 태그 수	50	아니요

AWS Config 규칙

설명	제한 값	높일 수 있음
계정당 리전당 최대 AWS Config 규칙 수	1000	아니요

단일 계정 적합성 팩

설명	제한 값	높일 수 있음
계정당 최대 적합성 팩 수	50	아니요
적합성 팩당 최대 AWS Config 규칙 수	130	아니요

> **Note**
> AWS Config 적합성 팩의 규칙은 계정당 리전당 최대 AWS Config 규칙 수 한도에 포함됩니다.

조직 적합성 팩

설명	제한 값	높일 수 있음
조직당 최대 적합성 팩 수	50	아니요
조직 적합성 팩당 최대 AWS Config 규칙 수	130	아니요

> **Note**
> 조직 수준에서를 배포하면 하위 계정의 한도에 포함됩니다.적합성 팩의 AWS Config 규칙은 계정당 리전당 최대 AWS Config 규칙 수 한도에 포함됩니다.

집계자

설명	제한 값	높일 수 있음
최대 구성 집계기 수	50	예
집계기의 최대 계정 수	10000	아니요
모든 집계기에 대해 주당 추가 또는 삭제된 최대 계정 수	1000	예

> **Note**
> 조직 수준 집계자와 개별 계정 집계자는 모두 최대 구성 집계자 수 제한에 포함됩니다.

고급 쿼리

설명	제한 값	높일 수 있음
단일 계정 및 리전에 저장된 최대 쿼리 수	300	예

에 대한 보충 정보 및 관련 리소스 AWS Config

다음의 관련 리소스는 이 서비스 사용 시 도움이 될 수 있습니다.

- AWS Config -에 대한 정보를 제공하는 기본 웹 페이지입니다 AWS Config.
- AWS Config 요금
- 기술 FAQ
- AWS Config 규칙 개발 키트(RDK) - 다양한 AWS 리소스 유형을 사용하여 규칙을 설정, 작성 및 테스트하는 데 도움이 AWS Config되는 오픈 소스 도구입니다.
- 파트너 - 구성 스트림, 구성 스냅샷 또는 구성 기록의 데이터를 시각화, 모니터링 및 관리하는 AWS Config 데 도움이 되도록와 완전히 통합된 파트너 제품에 대한 링크입니다.

- 클래스 및 워크숍 - AWS 기술을 연마하고 실용적인 경험을 얻는 데 도움이 되는 자기 주도형 랩 외에도 역할 기반 및 특수 과정으로 연결되는 링크입니다.
- AWS 개발자 센터 - 자습서를 살펴보고, 도구를 다운로드하고, AWS 개발자 이벤트에 대해 알아봅니다.
- AWS 개발자 도구 - AWS 애플리케이션 개발 및 관리를 위한 개발자 도구, SDKs, IDE 도구 키트 및 명령줄 도구에 대한 링크입니다.
- 리소스 센터 시작하기 -를 설정하고 AWS 계정, AWS 커뮤니티에 가입하고, 첫 번째 애플리케이션을 시작하는 방법을 알아봅니다.
- 실습 튜토리얼 – 단계별 튜토리얼에 따라 AWS에서 첫 번째 애플리케이션을 시작합니다.
- AWS 백서 - 아키텍처, 보안 및 경제와 같은 주제를 다루고 Solutions Architects 또는 기타 기술 전문가가 작성한 AWS 포괄적인 기술 AWS 백서 목록으로 연결되는 링크입니다.
- AWS Support 센터 - AWS Support 사례를 생성하고 관리하기 위한 허브입니다. 포럼, 기술 FAQs, 서비스 상태 및 같은 기타 유용한 리소스에 대한 링크도 포함되어 있습니다 AWS Trusted Advisor.
- 지원 - 클라우드에서 애플리케이션을 구축하고 실행하는 데 도움이 지원되는 one-on-one 빠른 응답 지원 채널에 대한 정보를 제공하는 기본 웹 페이지입니다.
- Contact Us(문의처) - AWS 결제, 계정, 이벤트, 침해 및 기타 문제에 대해 문의할 수 있는 중앙 연락 창구입니다.
- AWS 사이트 약관 - 저작권 및 상표, 계정, 라이선스 및 사이트 액세스, 기타 주제에 대한 자세한 정보입니다.

AWS 용 소프트웨어 개발 키트 AWS Config

AWS 소프트웨어 개발 키트(SDK)를 사용하면 비용 효율적이고 확장 가능하며 안정적인 AWS 인프라 서비스에 액세스하는 애플리케이션을 더 쉽게 구축할 수 있습니다. AWS SDK를 통해 라이브러리, 코드 샘플, 참조 설명서가 포함된 다운로드 가능한 단일 패키지로 몇 분 안에 시작할 수 있습니다. 다음 표에는 AWS Config 프로그래밍 방식으로에 액세스하는 데 사용할 수 있는 SDKs 및 타사 라이브러리가 나열되어 있습니다.

액세스 유형	설명
AWS SDKs	AWS 는 다음 SDKs • AWS SDK for C++ 설명서 • AWS Mobile SDK for iOS 설명서 • Go용AWS SDK 설명서 • AWS SDK for Java 설명서 • AWS SDK for JavaScript 설명서 • AWS SDK for .NET 설명서 • AWS SDK for PHP 설명서 • AWS SDK for Python (Boto) 설명서 • AWS SDK for Ruby 설명서
타사 라이브러리	AWS 개발자 커뮤니티의 개발자는 자체 라이브러리도 제공합니다. 라이브러리는 다음 AWS 개발자 센터에서 찾을 수 있습니다. • AWS Java 개발자 센터 • AWS JavaScript 개발자 센터 • AWS PHP 개발자 센터 • AWS Python 개발자 센터 • AWS Ruby 개발자 센터 • AWS Windows 및 .NET 개발자 센터

시작하기 AWS Config

AWS Config 는의 AWS 리소스 구성에 대한 자세한 보기를 제공합니다 AWS 계정. 를 사용하면 AWS 리소스 간 구성 및 관계의 변경 사항을 검토하고, 리소스 구성 기록을 탐색하고, 규칙을 사용하여 규정 준수를 확인할 AWS Config수 있습니다. 자세한 내용은 란 무엇입니까 AWS Config? 및 AWS Config 작동 방식을 참조하세요.

에 가입 AWS

주제

- 에 가입 AWS 계정
- 관리자 액세스 권한이 있는 사용자 생성

에 가입 AWS 계정

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   가입 절차의 일부로는 전화 또는 문자 메시지를 수신하고 전화 키패드에 확인 코드를 입력하는 것이 포함됩니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 AWS 계정보호 AWS IAM Identity Center, AWS 계정 루트 사용자활성화 및 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자AWS Management Console로에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 자격 증명 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 사용 AWS IAM Identity Center 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

를 시작하는 방법 AWS Config

에 가입한 후 AWS 계정, AWS Management Console AWS CLI 또는 SDK를 AWS Config 사용하여를 시작할 수 있습니다. AWS SDKs

- 콘솔 AWS Config 로 설정
- 를 AWS Config 사용하여 설정 AWS CLI
- AWS SDK에서 AWS Config 서비스 사용

콘솔 AWS Config 로 설정

는 설정을 위한 빠르고 간소화된 프로세스를 AWS Management Console 제공합니다 AWS Config.

설정

콘솔 AWS Config 을 사용하여를 설정하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Config 콘솔을 처음 열거나 새 리전 AWS Config 에서 설정하는 경우 AWS Config 콘솔 페이지는 다음과 같습니다.

3. AWS 모범 사례에 AWS Config 따라 시작하려면 원클릭 설정을 선택합니다. 시작하기를 선택하여 더 자세한 설정 프로세스를 진행할 수도 있습니다.

주제

- 에 대한 원클릭 설정 AWS Config
- 에 대한 수동 설정 AWS Config

에 대한 원클릭 설정 AWS Config

AWS Config 원클릭 설정을 사용하면 수동 선택 횟수를 줄여 AWS Config 콘솔 고객의 시작 프로세스를 간소화할 수 있습니다. 설정 프로세스의 모든 수동 선택 사항은 수동 설정 페이지를 참조하세요.

원클릭 설정을 사용하여 콘솔 AWS Config 로 설정하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 원클릭 설정을 선택합니다.

설정 페이지에는 세 단계가 포함되지만 원클릭 설정 워크플로를 통해 자동으로 3단계(검토)로 이동합니다. 다음은 해당 절차에 대한 세부 설명입니다.

- 설정: AWS Config 콘솔이 리소스와 역할을 기록하는 방식을 선택하고 구성 기록 및 구성 스냅샷 파일이 전송되는 위치를 선택합니다.
- 규칙: AWS 리전 해당 지원 AWS Config 규칙의 경우이 단계를 사용하여 계정에 추가할 수 있는 초기 관리형 규칙을 구성할 수 있습니다. 설정 후 AWS Config 는 선택한 규칙을 기준으로 AWS 리소스를 평가합니다. 설정 후 계정에서 추가 규칙을 생성하고 기존 규칙을 업데이트할 수 있습니다.
- 검토: 설정 세부 정보를 확인합니다.

1단계: 설정

기록 전략

사용자 지정 가능한 재정의가 있는 모든 리소스 유형을 기록하는 옵션이 선택됩니다. AWS Config 는 이 리전에서 현재 및 향후 지원되는 모든 리소스 유형을 기록합니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.

- 기본 설정

  기본 기록 빈도는 계속으로 설정되어 있습니다. 즉,는 변경이 발생할 때마다 구성 변경을 지속적으로 AWS Config 기록합니다.

AWS Config 는 기록 빈도를 매일로 설정하는 옵션도 지원합니다. 설정 후 이 옵션을 선택하면 이전에 기록된 CI와 다른 경우에만 지난 24시간 동안의 리소스 최신 상태를 나타내는 구성 항목(CI)을 받게 됩니다. 자세한 내용은 기록 빈도를 참조하세요.

> **Note**
>
> AWS Firewall Manager 는 리소스를 모니터링하기 위해 지속적인 레코딩에 의존합니다. Firewall Manager를 사용하는 경우 기록 빈도를 계속으로 설정하는 것이 좋습니다.

- 설정 재정의 - 선택 사항

  선택적으로 설정 후 특정 리소스 유형의 기록 빈도를 재정의하거나 기록에서 특정 리소스 유형을 제외할 수 있습니다. 기본 설정을 재정의하려면 AWS Config 콘솔의 왼쪽 탐색 창에서 설정을 선택한 다음 편집을 선택합니다.

리소스 기록 시 고려 사항

높은 AWS Config 평가 수

다음 달과 비교할 때 AWS Config를 사용하여 처음 한 달을 기록하는 동안 계정에서 활동이 증가하는 것을 확인할 수 있습니다. 초기 부트스트래핑 프로세스 중에는가 기록 AWS Config 하도록 선택한 계정의 모든 리소스에 대한 평가를 AWS Config 실행합니다.

임시 워크로드를 실행 중인 경우 AWS Config 가 이러한 임시 리소스의 생성 및 삭제와 관련된 구성 변경을 기록하므로 활동이 증가할 수 있습니다. 임시 워크로드는 컴퓨팅 리소스를 필요할 때 로드 및 실행하는 일시적 사용입니다. 대표적인 예는 Amazon Elastic Compute Cloud(Amazon EC2) 스팟 인스턴스, Amazon EMR 작업, AWS Auto Scaling이 있습니다. 임시 워크로드 실행으로 인한 활동 증가를 방지하려면 구성 레코더가 이러한 리소스 유형을 기록하지 않도록 설정하거나 AWS Config 가 비활성화된 별도의 계정에서 이러한 유형의 워크로드를 실행하여 구성 기록 및 규칙 평가가 증가하지 않도록 할 수 있습니다.

글로벌 리소스 유형 | Aurora 글로벌 클러스터는 처음에 기록에 포함됨

`AWS::RDS::GlobalCluster` 리소스 유형은 구성 레코더가 활성화된 지원되는 모든 AWS Config 리전에 기록됩니다.

활성화된 모든 리전에서 `AWS::RDS::GlobalCluster`를 기록하지 않으려면 설정 후 이 리소스 유형을 기록에서 제외할 수 있습니다. 왼쪽 탐색 모음에서 설정을 선택한 다음 편집을 선택합니다. 편집에

서 기록 방법 섹션의 재정의 설정으로 이동하여 `AWS::RDS::GlobalCluster`를 선택한 다음 '기록에서 제외'를 선택합니다.

글로벌 리소스 유형 | IAM 리소스 유형은 처음에 기록에서 제외됨

'전역적으로 기록되는 모든 IAM 리소스 유형'은 비용 절감을 위해 처음에 기록에서 제외됩니다. 이 번들에는 IAM 사용자, 그룹, 역할 및 고객 관리형 정책이 포함됩니다. 재정의를 제거하고 이러한 리소스를 기록에 포함하려면 제거를 선택합니다.

또한 2022년 2월 이후에 AWS Config 가 지원되는 리전에서는 글로벌 IAM 리소스 유형(`AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role`, `AWS::IAM::Policy`)을 기록할 수 없습니다. 이러한 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.

데이터 거버넌스

이 섹션에서는 7년(2557일) 동안 데이터를 보존하기 위한 기본 AWS Config 데이터 보존 기간을 선택합니다.

기존 AWS Config 서비스 연결 역할 사용 옵션이 자동으로 선택되고 AWS Config 역할로 설정됩니다. 서비스 연결 역할은에서 사전 정의 AWS Config 하며 서비스에서 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

전달 방법

이 섹션에서는 사용자 계정에서 버킷 선택 옵션이 자동으로 선택됩니다. 이 항목은 기본적으로 `config-bucket-`*`accountid`* 형식으로 이름이 지정된 계정의 버킷으로 설정됩니다. 예를 들어 `config-bucket-012345678901`입니다. 해당 형식으로 생성된 버킷이 없는 경우 버킷이 자동으로 생성됩니다. 자체 버킷을 생성하려는 경우 Amazon Simple Storage Service 사용 설명서의 버킷 생성을 참조하세요.

S3 버킷에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 개요를 참조하세요.

2단계: 규칙

AWS 관리형 규칙에는 이 단계에서 선택된 규칙이 없습니다. 대신 계정 설정을 완료한 후 규칙을 생성하고 업데이트하는 것이 좋습니다.

3단계: 검토

AWS Config 설정 세부 정보를 검토합니다. 돌아가서 각 섹션을 편집할 수 있습니다. 확인을 선택하여 설정을 완료합니다 AWS Config.

에 대한 수동 설정 AWS Config

시작하기 워크플로를 사용하면 설정 프로세스의 모든 수동 선택을 통해 AWS Config 콘솔을 시작할 수 있습니다. 간소화된 시작 프로세스는 원클릭 설정을 참조하세요.

시작하기를 사용하여 콘솔 AWS Config 로 설정하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. Get started를 선택합니다.

설정 페이지에는 세 단계가 있습니다. 다음은 시작하기를 선택한 후의 절차에 대한 세부 설명입니다.

- 설정: AWS Config 콘솔이 리소스와 역할을 기록하는 방식을 선택하고 구성 기록 및 구성 스냅샷 파일이 전송되는 위치를 선택합니다.
- 규칙: AWS 리전 해당 지원 AWS Config 규칙의 경우이 단계를 사용하여 계정에 추가할 수 있는 초기 관리형 규칙을 구성할 수 있습니다. 설정 후 AWS Config 는 선택한 규칙을 기준으로 AWS 리소스를 평가합니다. 설정 후 계정에서 추가 규칙을 생성하고 기존 규칙을 업데이트할 수 있습니다.
- 검토: 설정 세부 정보를 확인합니다.

1단계: 설정

기록 전략

기록 방법 섹션에서 기록 전략을 선택합니다. 기록할 AWS 리소스를 지정할 수 AWS Config 있습니다.

All resource types with customizable overrides

이 리전에서 현재 및 향후 지원되는 모든 리소스 유형에 대한 구성 변경을 기록 AWS Config 하도록 설정합니다. 특정 리소스 유형의 기록 빈도를 재정의하거나 기록에서 특정 리소스 유형을 제외할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.

- 기본 설정

  현재 및 향후 지원되는 모든 리소스 유형에 대한 기본 기록 빈도를 구성합니다. 자세한 내용은 기록 빈도를 참조하세요.

  - 연속 기록 - 변경 AWS Config 사항이 발생할 때마다 구성 변경을 지속적으로 기록합니다.

- 일일 기록 - 이전에 기록된 CI와 다른 경우에만 지난 24시간 동안의 리소스 최신 상태를 나타내는 구성 항목(CI)을 받게 됩니다.

> **Note**
>
> AWS Firewall Manager 는 리소스를 모니터링하기 위해 지속적인 레코딩에 의존합니다. Firewall Manager를 사용하는 경우 기록 빈도를 계속으로 설정하는 것이 좋습니다.

- 설정 재정의

  특정 리소스 유형의 기록 빈도를 재정의하거나 기록에서 특정 리소스 유형을 제외합니다. 리소스 유형의 기록 빈도를 변경하거나 리소스 유형에 대한 기록을 중지하는 경우 이미 기록된 구성 항목은 변경되지 않습니다.

Specific resource types

지정한 리소스 유형에 대해서만 구성 변경을 기록 AWS Config 하도록 설정합니다.

- 특정 리소스 유형

  기록할 리소스 유형과 빈도를 선택합니다. 자세한 내용은 기록 빈도를 참조하세요.

  - 연속 기록 - 변경 AWS Config 사항이 발생할 때마다 구성 변경을 지속적으로 기록합니다.
  - 일일 기록 - 이전에 기록된 CI와 다른 경우에만 지난 24시간 동안의 리소스 최신 상태를 나타내는 구성 항목(CI)을 받게 됩니다.

> **Note**
>
> AWS Firewall Manager 는 리소스를 모니터링하기 위해 지속적인 레코딩에 의존합니다. Firewall Manager를 사용하는 경우 기록 빈도를 계속으로 설정하는 것이 좋습니다.

  리소스 유형의 기록 빈도를 변경하거나 리소스 유형에 대한 기록을 중지하는 경우 이미 기록된 구성 항목은 변경되지 않습니다.

리소스 기록 시 고려 사항

높은 AWS Config 평가 수

다음 달과 비교할 때 AWS Config를 사용하여 처음 한 달을 기록하는 동안 계정에서 활동이 증가하는 것을 확인할 수 있습니다. 초기 부트스트래핑 프로세스 중에는가 기록 AWS Config 하도록 선택한 계정의 모든 리소스에 대한 평가를 AWS Config 실행합니다.

임시 워크로드를 실행 중인 경우 AWS Config 가 이러한 임시 리소스의 생성 및 삭제와 관련된 구성 변경을 기록하므로 활동이 증가할 수 있습니다. 임시 워크로드는 컴퓨팅 리소스를 필요할 때 로드 및 실행하는 일시적 사용입니다. 예를 들면 Amazon Elastic Compute Cloud(Amazon EC2) 스팟 인스턴스, Amazon EMR 작업 및 등이 AWS Auto Scaling있습니다. 임시 워크로드 실행으로 인한 활동 증가를 방지하려면 구성 레코더가 이러한 리소스 유형을 기록하지 않도록 설정하거나 AWS Config 가 비활성화된 별도의 계정에서 이러한 유형의 워크로드를 실행하여 구성 기록 및 규칙 평가가 증가하지 않도록 할 수 있습니다.

Considerations: All resource types with customizable overrides

전역적으로 기록되는 리소스 유형 | Aurora 글로벌 클러스터는 처음에 기록에 포함됨

`AWS::RDS::GlobalCluster` 리소스 유형은 구성 레코더가 활성화된 지원되는 모든 AWS Config 리전에 기록됩니다.

활성화된 모든 리전에서 `AWS::RDS::GlobalCluster`를 기록하지 않으려면 ‘AWS RDS GlobalCluster’를 선택하고 ‘기록에서 제외’ 재정의를 선택합니다.

글로벌 리소스 유형 | IAM 리소스 유형은 처음에 기록에서 제외됨

글로벌 IAM 리소스 유형은 비용 절감을 위해 처음에 기록에서 제외됩니다. 이 번들에는 IAM 사용자, 그룹, 역할 및 고객 관리형 정책이 포함됩니다. 재정의를 제거하고 이러한 리소스를 기록에 포함하려면 제거를 선택합니다.

또한 글로벌 IAM 리소스 유형(`AWS::IAM::User`, `AWS::IAM::Role`, 및 `AWS::IAM::GroupAWS::IAM::Policy`)은 2022년 2월 AWS Config 이후에서 지원하는 리전에 기록할 수 없습니다. 이러한 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.

Limits

최대 100개의 빈도 재정의와 600개의 제외 재정의를 추가할 수 있습니다.

다음 리소스 유형에는 일일 기록을 지정할 수 없습니다.

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

리전 가용성

추적할 리소스 유형을 지정 AWS Config 하기 전에 리전 가용성별 리소스 적용 범위를 확인하여 설정한 AWS 리전에서 리소스 유형이 지원되는지 확인합니다 AWS Config. 리소스 유형이 하나 이상의 리전 AWS Config 에서에서 지원되는 경우, 설정한 리전에서 AWS Config지정된 리소스 유형이 지원되지 않더라도에서 지원하는 모든 AWS 리전에서 해당 리소스 유형의 기록을 활성화할 수 있습니다 AWS Config.

Limits

모든 리소스 유형의 빈도가 같으면 제한이 없습니다. 하나 이상의 리소스 유형이 계속으로 설정된 경우 일일 빈도를 사용하여 최대 100개의 리소스 유형을 추가할 수 있습니다.

다음과 같은 리소스 유형에는 일일 빈도가 지원되지 않습니다.

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

데이터 거버넌스

- 데이터 보존 기간에서 기본 보존 기간을 선택하여 7년(2557) 동안 AWS Config 데이터를 보존하거나에서 기록한 항목에 대한 사용자 지정 임대 기간을 설정합니다 AWS Config.

  AWS Config 를 사용하면의 보존 기간을 지정하여 데이터를 삭제할 수 있습니다`ConfigurationItems`. 보존 기간을 지정하면, AWS Config 는 이 지정된 기간 동안 `ConfigurationItems`을 유지합니다. 최소 30일에서 최대 7년(2557일) 사이의 기간을 선택할 수 있습니다.는 지정된 보존 기간보다 오래된 데이터를 AWS Config 삭제합니다.
- 에 대한 IAM 역할 AWS Config의 경우 계정에서 기존 AWS Config 서비스 연결 역할 또는 IAM 역할을 선택합니다.
  - 서비스 연결 역할은에서 사전 정의 AWS Config 하며 서비스에서 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

> **Note**
>
> 권장 사항: 서비스 연결 역할 사용

서비스 연결 역할을 사용하는 것이 좋습니다. 서비스 연결 역할은 AWS Config 을 예상대로 실행하는 데 필요한 모든 권한을 추가합니다.

- 또는 기존 역할 및 권한 정책 중 하나에서 IAM 역할을 선택합니다.

> **Note**
>
> 정책 및 규정 준수 결과
> 에서 관리되는 IAM 정책 및 기타 정책은 AWS Config 에 리소스에 대한 구성 변경을 기록할 권한이 있는지 여부에 영향을 미칠 수 있습니다. AWS Organizations 또한 규칙은 리소스의 구성을 직접 평가하며, 규칙은 평가를 실행할 때 이러한 정책을 고려하지 않습니다. 적용 중인 정책이 사용 의도와 일치하는지 확인합니다 AWS Config.
> IAM 역할 재사용 시 최소 권한 유지
> 또는 AWS Control Tower와 AWS Config같이 AWS Security Hub 에서 사용하는 AWS 서비스를 사용하고 IAM 역할이 이미 생성된 경우 설정 AWS Config 시 사용하는 IAM 역할이 기존 IAM 역할과 동일한 최소 권한을 유지하는지 확인합니다. 다른 AWS 서비스가 예상대로 계속 실행되도록 하려면이 작업을 수행해야 합니다.
> 예를 들어 AWS Control Tower 에 S3 객체를 읽을 AWS Config 수 있는 IAM 역할이 있는 경우 설정 시 사용하는 IAM 역할에 동일한 권한이 부여되었는지 확인합니다 AWS Config. 그렇지 않으면 AWS Control Tower 운영에 방해가 될 수 있습니다.

전달 방법

- 전달 방법에서 AWS Config 가 구성 이력 및 구성 스냅샷 파일을 보낼 S3 버킷을 선택합니다.
  - 버킷 생성 - S3 버킷 이름에 S3 버킷의 이름을 입력합니다.

    입력하는 이름은 Amazon S3에 있는 기존 버킷 이름을 모두 통틀어 고유해야 합니다. 고유성을 유지하기 위한 한 가지 방법은 접두사(예: 조직 이름)를 포함시키는 것입니다. 버킷을 만든 후에는 버킷 이름을 변경할 수 없습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 규제 및 제한을 참조하세요.
  - 계정에서 버킷 선택 - S3 버킷 이름에서 선호하는 버킷을 선택합니다.
  - 다른 계정에서 버킷 선택 - S3 버킷 이름에 버킷 이름을 입력합니다.

> **Note**
>
> 버킷 권한

다른 계정에서 버킷을 선택하는 경우 해당 버킷에는 액세스 권한을 부여하는 정책이 있어야 합니다 AWS Config. 자세한 내용은 AWS Config 전송 채널에 대한 Amazon S3 버킷에 대한 권한 단원을 참조하십시오.

- Amazon SNS 주제에서 구성 기록 전송, 구성 스냅샷 전송 및 규정 준수와 같은 알림을 보내려면 Amazon SNS 주제에 대한 구성 변경 사항 및 알림 스트리밍을 선택합니다. AWS Config
- Amazon SNS 주제로 AWS Config 스트리밍하도록 선택한 경우 대상 주제를 선택합니다.
  - 주제 생성 - 주제 이름에 SNS 주제의 이름을 입력합니다.
  - 계정에서 주제 선택 - 주제 이름에서 원하는 주제를 선택합니다.
  - 다른 계정에서 주제 선택 - 주제 ARN에 주제의 Amazon 리소스 이름(ARN)을 입력합니다. 다른 계정에서 주제를 선택하는 경우 주제에 액세스 권한을 부여하는 정책이 있어야 합니다 AWS Config. 자세한 내용은 Amazon SNS 주제에 대한 권한 단원을 참조하십시오.

> **Note**
>
> Amazon SNS 주제의 리전
> Amazon SNS 주제는 설정한 리전과 동일한 리전에 있어야 합니다 AWS Config.

2단계: 규칙

규칙을 지원하는 리전 AWS Config 에서를 설정하는 경우 다음을 선택합니다.

3단계: 검토

AWS Config 설정 세부 정보를 검토합니다. 돌아가서 각 섹션을 편집할 수 있습니다. 확인을 선택하여 설정을 완료합니다 AWS Config.

자세한 정보

계정에서 기존 리소스를 검색하고 리소스 구성을 파악하는 방법에 대한 자세한 내용은 리소스 검색, 규정 준수 정보 보기 및 규정 준수 기록 보기를 참조하세요.

Amazon Simple Queue Service를 사용하여 프로그래밍 방식으로 AWS 리소스를 모니터링할 수도 있습니다. 자세한 내용은 Amazon SQS를 사용하여 AWS 리소스 변경 모니터링 단원을 참조하십시오.

를 AWS Config 사용하여 설정 AWS CLI

AWS CLI 는 AWS 서비스를 관리하기 위한 통합 도구입니다. 다운로드 및 구성할 도구를 하나만 사용하면 명령줄에서 여러 AWS 서비스를 제어하고 스크립트를 사용하여 자동화할 수 있습니다. AWS CLI 및에 대한 자세한 내용과 AWS CLI 도구 설치 지침은 AWS Command Line Interface 사용 설명서의 다음을 참조하세요.

- AWS Command Line Interface 사용 설명서
- AWS Command Line Interface를 이용한 설정

필요한 경우 `aws configure`를 입력하여 AWS Config 가 사용 가능한 리전을 AWS CLI AWS 사용하도록 구성합니다.

설정

를 사용하여 설정하려면 다음 주제를 참조 AWS Config 하세요 AWS CLI.

주제

- 를 AWS Config 사용하여 설정하기 위한 사전 조건 AWS CLI
- 를 사용하여 고객 관리형 구성 레코더 AWS Config 로 시작 AWS CLI
- 이 로 성공적으로 시작 AWS Config 되었는지 확인 AWS CLI

를 AWS Config 사용하여 설정하기 위한 사전 조건 AWS CLI

AWS 로 설정하기 전에 사전 조건으로 정책이 연결된 Amazon S3 버킷, Amazon SNS 주제 및 IAM 역할을 생성 AWS CLI해야 합니다. 그런 다음 AWS CLI 를 사용하여 버킷, 주제 및 역할을 지정할 수 있습니다 AWS Config. 이 절차에 따라 AWS Config사전 조건을 설정하세요.

주제

- 1단계: Amazon S3 버킷 생성
- 2단계: Amazon SNS 주제 생성
- 3단계: IAM 역할 생성

1단계: Amazon S3 버킷 생성

계정에 이미 있는 Amazon S3 버킷을 사용하려면 이 단계를 건너뛰고 2단계: Amazon SNS 주제 생성 섹션으로 이동합니다.

S3 콘솔 사용

버킷을 생성하려면

1. https://console.aws.amazon.com/s3/에서 Amazon S3 콘솔을 엽니다.
2. 버킷 생성을 선택합니다.
3. 버킷 이름에 버킷의 DNS 호환 이름을 입력합니다.

   버킷 이름은 다음과 같아야 합니다.

   - 모든 Amazon S3에서 고유해야 합니다.
   - 3~63자 이내여야 합니다.
   - 대문자가 없어야 합니다.
   - 소문자 또는 숫자로 시작해야 합니다.

   버킷을 생성한 후에는 해당 이름을 변경할 수 없습니다. 선택하는 버킷 이름은 Amazon S3의 모든 기존 버킷 이름을 통틀어 고유해야 합니다. 버킷 명명 규칙에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 안내서의 버킷 규제 및 제한을 참조하세요.

   > **Important**
   > 버킷 이름에 민감한 정보를 포함하지 마세요. 버킷 이름은 버킷의 객체를 가리키는 URL에 표시됩니다.

4. 리전에서 버킷이 상주할 AWS 리전을 선택합니다.

   가까운 리전을 선택하면 지연 시간과 요금을 최소화하고 규제 요건을 다룰 수 있습니다. 특정 리전에 저장된 객체는 사용자가 명시적으로 객체를 다른 리전으로 전송하지 않는 한 해당 리전을 벗어나지 않습니다. Amazon S3 AWS Regions 목록은의 AWS 서비스 엔드포인트를 참조하세요Amazon Web Services 일반 참조.

5. Bucket settings for Block Public Access(퍼블릭 액세스 차단을 위한 버킷 설정)에서 버킷에 적용할 퍼블릭 액세스 차단 설정을 선택합니다.

퍼블릭 웹 사이트 호스팅과 같은 사용 사례에 대해 하나 이상의 설정을 해제해야 하는 경우가 아니면 모든 설정을 사용하도록 설정하는 것이 좋습니다. 버킷에 대해 활성화한 퍼블릭 액세스 차단 설정도 버킷에 생성한 모든 액세스 포인트에 대해 활성화됩니다. 퍼블릭 액세스 차단에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 퍼블릭 액세스 차단 사용을 참조하세요.

6. (선택 사항) S3 객체 잠금을 활성화하려면 다음을 수행합니다.

   a. 고급 설정을 선택하고 나타나는 메시지를 읽습니다.

   > **Important**
   >
   > 버킷을 생성할 때만 S3 객체 잠금을 활성화할 수 있습니다. 버킷에 대해 객체 잠금을 활성화하면 나중에 비활성화할 수 없습니다. 객체 잠금을 활성화하면 버킷의 버전 관리도 활성화됩니다. 버킷에 대해 객체 잠금을 활성화한 후 객체 잠금 설정을 구성해야 버킷의 객체가 보호됩니다. 객체의 보호 구성에 대한 자세한 내용은 Amazon S3 콘솔을 사용하여 S3 객체 잠금 구성을 참조하세요.

   b. 객체 잠금을 활성화하려면 텍스트 상자에 enable을 입력하고 확인(Confirm)을 선택합니다.

   S3 객체 잠금 기능에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 객체 잠금을 사용하여 객체 잠금을 참조하세요.

7. 버킷 생성을 선택합니다.

AWS SDKs 사용

AWS SDKs를 사용하여 버킷을 생성하는 경우 클라이언트를 생성한 다음 클라이언트를 사용하여 버킷 생성 요청을 보내야 합니다. 모범 사례로서, 동일한 AWS 리전에 클라이언트 및 버킷을 만들어야 합니다. 클라이언트나 버킷을 생성할 때 리전을 지정하지 않으면 Amazon S3는 기본 리전인 미국 동부(버지니아 북부)를 사용합니다.

듀얼 스택 엔드포인트에 액세스할 클라이언트를 생성하려면를 지정해야 합니다 AWS 리전. 자세한 내용은 Amazon S3 듀얼 스택 엔드포인트를 참조하세요. 사용 가능한 목록은의 리전 및 엔드포인트를 AWS 리전참조하세요AWS 일반 참조.

클라이언트를 만들면 리전은 리전별 엔드포인트로 매핑됩니다. 클라이언트는 `s3.<region>.amazonaws.com` 엔드포인트를 사용하여 Amazon S3와 통신합니다. 2019년 3월 20일 이후에 리전이 시작된 경우 클라이언트와 버킷이 동일한 리전에 있어야 합니다. 다만 미국 동부(버

지니아 북부) 리전의 클라이언트를 사용하면 2019년 3월 20일 이전에 시작된 모든 리전에 버킷을 생성할 수 있습니다. 자세한 내용은 레거시 엔드포인트를 참조하세요.

이러한 AWS SDK 코드 예제는 다음 작업을 수행합니다.

- AWS 리전을 명시적으로 지정하여 클라이언트 생성 - 이 예에서 클라이언트는 `s3.us-west-2.amazonaws.com` 엔드포인트를 사용하여 Amazon S3와 통신합니다. AWS 리전을 지정할 수 있습니다. 목록은 AWS 일반 AWS 리전참조의 리전 및 엔드포인트를 참조하세요.
- 버킷 이름만 지정하여 버킷 생성 요청 전송 - 클라이언트는 Amazon S3로 요청을 전송하여 클라이언트가 생성된 리전에 버킷을 생성합니다.
- 버킷의 위치에 대한 정보 검색 - Amazon S3는 버킷과 연결된 location 하위 리소스에 버킷 위치 정보를 저장합니다.

다음 코드 예시는 `CreateBucket`의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
        /// <summary>
        /// Shows how to create a new Amazon S3 bucket.
        /// </summary>
        /// <param name="client">An initialized Amazon S3 client object.</param>
        /// <param name="bucketName">The name of the bucket to create.</param>
        /// <returns>A boolean value representing the success or failure of
        /// the bucket creation process.</returns>
        public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string
bucketName)
        {
            try
            {
                var request = new PutBucketRequest
                {
```

```
                    BucketName = bucketName,
                    UseClientRegion = true,
                };

                var response = await client.PutBucketAsync(request);
                return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
            }
            catch (AmazonS3Exception ex)
            {
                Console.WriteLine($"Error creating bucket: '{ex.Message}'");
                return false;
            }
        }
```

객체 잠금을 활성화한 버킷을 생성합니다.

```
    /// <summary>
    /// Create a new Amazon S3 bucket with object lock actions.
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
    /// <param name="enableObjectLock">True to enable object lock on the
bucket.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateBucketWithObjectLock(string bucketName, bool
enableObjectLock)
    {
        Console.WriteLine($"\tCreating bucket {bucketName} with object lock
{enableObjectLock}.");
        try
        {
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
```

```
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 CreateBucket을 참조하세요.

Bash

AWS CLI Bash 스크립트 사용

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
```

```
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally
 unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
```

```
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi

  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- API 세부 정보는 AWS CLI 명령 참조의 CreateBucket을 참조하세요.

C++

SDK for C++

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
bool AwsDoc::S3::createBucket(const Aws::String &bucketName,
                              const Aws::S3::S3ClientConfiguration &clientConfig)
 {
    Aws::S3::S3Client client(clientConfig);
    Aws::S3::Model::CreateBucketRequest request;
    request.SetBucket(bucketName);

    if (clientConfig.region != "us-east-1") {
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

 Aws::S3::Model::BucketLocationConstraintMapper::GetBucketLocationConstraintForName(
                        clientConfig.region));
        request.SetCreateBucketConfiguration(createBucketConfig);
    }

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
        auto err = outcome.GetError();
        std::cerr << "Error: createBucket: " <<
                  err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    } else {
        std::cout << "Created bucket " << bucketName <<
                  " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- API 세부 정보는 AWS SDK for C++ API 참조의 CreateBucket을 참조하세요.

CLI

AWS CLI

예 1: 버킷을 생성하는 방법

다음 `create-bucket` 예시에서는 `amzn-s3-demo-bucket`이라는 버킷을 생성합니다.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1
```

출력:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

자세한 내용은 Amazon S3 사용자 안내서의 버킷 생성을 참조하세요.

예시 2: 소유자가 적용된 버킷 생성

다음 `create-bucket` 예시에서는 S3 객체 소유권에 대해 버킷 소유자 적용 설정을 사용하는 `amzn-s3-demo-bucket`이라는 버킷을 생성합니다.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

출력:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

자세한 내용은 Amazon S3 사용자 안내서의 객체 소유권 제어 및 ACL 비활성화를 참조하세요.

예시 3: 'us-east-1' 리전 외부에서 버킷 생성

다음 `create-bucket` 예시에서는 `eu-west-1` 리전에서 `amzn-s3-demo-bucket`이라는 버킷을 생성합니다. `us-east-1` 외부 리전의 경우 원하는 리전에 버킷을 생성하려면 적절한 `LocationConstraint`를 지정해야 합니다.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

출력:

```
{
    "Location": "http://amzn-s3-demo-bucket.s3.amazonaws.com/"
}
```

자세한 내용은 Amazon S3 사용자 안내서의 버킷 생성을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 CreateBucket을 참조하세요.

Go

SDK for Go V2

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

기본 구성으로 버킷을 생성합니다.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "io"
 "log"
 "os"
 "time"
```

```
 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(ctx context.Context, name string, region
 string) error {
 _, err := basics.S3Client.CreateBucket(ctx, &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", name)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", name)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(basics.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(name)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", name)
```

```
  }
 }
 return err
}
```

객체 잠금 기능이 있는 버킷을 만들고 버킷이 존재할 때까지 기다립니다.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// S3Actions wraps S3 service actions.
type S3Actions struct {
 S3Client  *s3.Client
 S3Manager *manager.Uploader
}



// CreateBucketWithLock creates a new S3 bucket with optional object locking
 enabled
// and waits for the bucket to exist before returning.
func (actor S3Actions) CreateBucketWithLock(ctx context.Context, bucket string,
 region string, enableObjectLock bool) (string, error) {
 input := &s3.CreateBucketInput{
  Bucket: aws.String(bucket),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
```

```
 }

 if enableObjectLock {
  input.ObjectLockEnabledForBucket = aws.Bool(true)
 }

 _, err := actor.S3Client.CreateBucket(ctx, input)
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", bucket)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", bucket)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(actor.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(bucket)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", bucket)
  }
 }

 return bucket, err
}
```

- API 세부 정보는 AWS SDK for Go API 참조의 CreateBucket을 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

버킷을 만듭니다.

```
   /**
    * Creates an S3 bucket asynchronously.
    *
    * @param bucketName the name of the S3 bucket to create
    * @return a {@link CompletableFuture} that completes when the bucket is
created and ready
    * @throws RuntimeException if there is a failure while creating the bucket
    */
   public CompletableFuture<Void> createBucketAsync(String bucketName) {
       CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
           .bucket(bucketName)
           .build();

       CompletableFuture<CreateBucketResponse> response =
getAsyncClient().createBucket(bucketRequest);
       return response.thenCompose(resp -> {
           S3AsyncWaiter s3Waiter = getAsyncClient().waiter();
           HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
               .bucket(bucketName)
               .build();

           CompletableFuture<WaiterResponse<HeadBucketResponse>>
waiterResponseFuture =
               s3Waiter.waitUntilBucketExists(bucketRequestWait);
           return waiterResponseFuture.thenAccept(waiterResponse -> {
               waiterResponse.matched().response().ifPresent(headBucketResponse
-> {
                   logger.info(bucketName + " is ready");
               });
           });
       }).whenComplete((resp, ex) -> {
           if (ex != null) {
               throw new RuntimeException("Failed to create bucket", ex);
           }
       });
   }
```

객체 잠금을 활성화한 버킷을 생성합니다.

```
    // Create a new Amazon S3 bucket with object lock options.
    public void createBucketWithLockOptions(boolean enableObjectLock, String
 bucketName) {
        S3Waiter s3Waiter = getClient().waiter();
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectLockEnabledForBucket(enableObjectLock)
            .build();

        getClient().createBucket(bucketRequest);
        HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
            .bucket(bucketName)
            .build();

        // Wait until the bucket is created and print out the response.
        s3Waiter.waitUntilBucketExists(bucketRequestWait);
        System.out.println(bucketName + " is ready");
    }
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 CreateBucket을 참조하세요.

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

버킷을 생성합니다.

```
import {
  BucketAlreadyExists,
  BucketAlreadyOwnedByYou,
  CreateBucketCommand,
  S3Client,
  waitUntilBucketExists,
} from "@aws-sdk/client-s3";
```

```
/**
 * Create an Amazon S3 bucket.
 * @param {{ bucketName: string }} config
 */
export const main = async ({ bucketName }) => {
  const client = new S3Client({});

  try {
    const { Location } = await client.send(
      new CreateBucketCommand({
        // The name of the bucket. Bucket names are unique and have several other
 constraints.
        // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
        Bucket: bucketName,
      }),
    );
    await waitUntilBucketExists({ client }, { Bucket: bucketName });
    console.log(`Bucket created with location ${Location}`);
  } catch (caught) {
    if (caught instanceof BucketAlreadyExists) {
      console.error(
        `The bucket "${bucketName}" already exists in another AWS account. Bucket
 names must be globally unique.`,
      );
    }
    // WARNING: If you try to create a bucket in the North Virginia region,
    // and you already own a bucket in that region with the same name, this
    // error will not be thrown. Instead, the call will return successfully
    // and the ACL on that bucket will be reset.
    else if (caught instanceof BucketAlreadyOwnedByYou) {
      console.error(
        `The bucket "${bucketName}" already exists in this AWS account.`,
      );
    } else {
      throw caught;
    }
  }
};
```

- 자세한 정보는 AWS SDK for JavaScript 개발자 안내서를 참조하세요.

- API 세부 정보는 AWS SDK for JavaScript API 참조의 CreateBucket을 참조하세요.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun createNewBucket(bucketName: String) {
    val request =
        CreateBucketRequest {
            bucket = bucketName
        }

    S3Client { region = "us-east-1" }.use { s3 ->
        s3.createBucket(request)
        println("$bucketName is ready")
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 CreateBucket를 참조하세요.

PHP

SDK for PHP

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

버킷을 만듭니다.

```
        $s3client = new Aws\S3\S3Client(['region' => 'us-west-2']);
```

```
        try {
            $this->s3client->createBucket([
                'Bucket' => $this->bucketName,
                'CreateBucketConfiguration' => ['LocationConstraint' => $region],
            ]);
            echo "Created bucket named: $this->bucketName \n";
        } catch (Exception $exception) {
            echo "Failed to create bucket $this->bucketName with error: " .
 $exception->getMessage();
            exit("Please fix error with bucket creation before continuing.");
        }
```

- API 세부 정보는 AWS SDK for PHP API 참조의 CreateBucket을 참조하세요.

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

기본 설정으로 버킷을 생성합니다.

```
class BucketWrapper:
    """Encapsulates S3 bucket actions."""

    def __init__(self, bucket):
        """
        :param bucket: A Boto3 Bucket resource. This is a high-level resource in
 Boto3
                       that wraps bucket actions in a class-like structure.
        """
        self.bucket = bucket
        self.name = bucket.name


    def create(self, region_override=None):
```

```
        """
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

        :param region_override: The Region in which to create the bucket. If this
 is
                                not specified, the Region configured in your
 shared
                                credentials is used.
        """
        if region_override is not None:
            region = region_override
        else:
            region = self.bucket.meta.client.meta.region_name
        try:
            self.bucket.create(CreateBucketConfiguration={"LocationConstraint":
 region})

            self.bucket.wait_until_exists()
            logger.info("Created bucket '%s' in region=%s", self.bucket.name,
 region)
        except ClientError as error:
            logger.exception(
                "Couldn't create bucket named '%s' in region=%s.",
                self.bucket.name,
                region,
            )
            raise error
```

수명 주기 구성으로 버전이 지정된 버킷을 생성합니다.

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.
```

```
    Usage is shown in the usage_demo_single_object function at the end of this
module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
```

```
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 CreateBucket를 참조하세요.

Ruby

SDK for Ruby

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
```

```
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

- API 세부 정보는 AWS SDK for Ruby API 참조의 CreateBucket을 참조하세요.

Rust

SDK for Rust

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
pub async fn create_bucket(
    client: &aws_sdk_s3::Client,
    bucket_name: &str,
    region: &aws_config::Region,
) -> Result<Option<aws_sdk_s3::operation::create_bucket::CreateBucketOutput>,
 S3ExampleError> {
    let constraint =
 aws_sdk_s3::types::BucketLocationConstraint::from(region.to_string().as_str());
    let cfg = aws_sdk_s3::types::CreateBucketConfiguration::builder()
        .location_constraint(constraint)
        .build();
    let create = client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await;

    // BucketAlreadyExists and BucketAlreadyOwnedByYou are not problems for this
 task.
    create.map(Some).or_else(|err| {
        if err
            .as_service_error()
            .map(|se| se.is_bucket_already_exists() ||
 se.is_bucket_already_owned_by_you())
            == Some(true)
        {
            Ok(None)
```

```
        } else {
            Err(S3ExampleError::from(err))
        }
    })
}
```

- API 세부 정보는 AWS SDK for Rust API 참조의 CreateBucket을 참조하세요.

SAP ABAP

SDK for SAP ABAP API

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    TRY.
        " determine our region from our session
        DATA(lv_region) = CONV /aws1/s3_bucketlocationcnstrnt( lo_session-
>get_region( ) ).
        DATA lo_constraint TYPE REF TO /aws1/cl_s3_createbucketconf.
        " When in the us-east-1 region, you must not specify a constraint
        " In all other regions, specify the region as the constraint
        IF lv_region = 'us-east-1'.
          CLEAR lo_constraint.
        ELSE.
          lo_constraint = NEW /aws1/cl_s3_createbucketconf( lv_region ).
        ENDIF.

        lo_s3->createbucket(
            iv_bucket = iv_bucket_name
            io_createbucketconfiguration  = lo_constraint ).
        MESSAGE 'S3 bucket created.' TYPE 'I'.
      CATCH /aws1/cx_s3_bucketalrdyexists.
        MESSAGE 'Bucket name already exists.' TYPE 'E'.
      CATCH /aws1/cx_s3_bktalrdyownedbyyou.
        MESSAGE 'Bucket already exists and is owned by you.' TYPE 'E'.
    ENDTRY.
```

- API 세부 정보는AWS SDK for SAP ABAP API의 CreateBucket을 참조하세요.

Swift

SDK for Swift

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import AWSS3

    public func createBucket(name: String) async throws {
        var input = CreateBucketInput(
            bucket: name
        )

        // For regions other than "us-east-1", you must set the
 locationConstraint in the createBucketConfiguration.
        // For more information, see LocationConstraint in the S3 API guide.
        // https://docs.aws.amazon.com/AmazonS3/latest/API/
API_CreateBucket.html#API_CreateBucket_RequestBody
        if let region = configuration.region {
            if region != "us-east-1" {
                input.createBucketConfiguration =
 S3ClientTypes.CreateBucketConfiguration(locationConstraint:
 S3ClientTypes.BucketLocationConstraint(rawValue: region))
            }
        }

        do {
            _ = try await client.createBucket(input: input)
        }
        catch let error as BucketAlreadyOwnedByYou {
            print("The bucket '\(name)' already exists and is owned by you. You
 may wish to ignore this exception.")
            throw error
        }
```

```
        catch {
            print("ERROR: ", dump(error, name: "Creating a bucket"))
            throw error
        }
    }
```

- API 세부 정보는 AWS SDK for Swift API 참조의 CreateBucket을 참조하세요.

> **Note**
>
> 다른 계정의 Amazon S3 버킷을 사용할 수도 있으나, 해당 버킷에 대해 AWS Config에 액세스 권한을 부여하는 정책을 생성해야 할 수 있습니다. Amazon S3 버킷에 권한을 부여하는 방법에 대한 자세한 내용은 AWS Config 전송 채널에 대한 Amazon S3 버킷에 대한 권한 섹션을 참조한 후 2단계: Amazon SNS 주제 생성 섹션으로 이동하세요.

2단계: Amazon SNS 주제 생성

계정에 이미 있는 Amazon SNS 주제를 사용하려면 이 단계를 건너뛰고 3단계: IAM 역할 생성 섹션으로 이동합니다.

SNS 콘솔 사용

Amazon SNS 토픽을 생성하려면

1. https://console.aws.amazon.com/sns/v3/home에서 Amazon SNS 콘솔을 엽니다.
2. 다음 중 하나를 수행합니다.
   - AWS 계정 이전에에서 생성된 주제가 없는 경우 홈 페이지에서 Amazon SNS에 대한 설명을 읽습니다.
   - AWS 계정 이전에에서 주제를 생성한 경우 탐색 패널에서 주제를 선택합니다.
3. 주제 페이지에서 주제 생성을 선택합니다.
4. 주제 생성 페이지의 세부 정보 섹션에서 다음을 수행합니다.
   a. 유형에서 주제 유형(표준 또는 FIFO을 선택합니다.
   b. 주제의 이름을 입력합니다. FIFO 주제의 경우 이름 끝에 .fifo를 추가합니다.

c. (선택 사항) 주제의 표시 이름을 입력합니다.

d. (선택 사항) FIFO 주제의 경우 콘텐츠 기반 메시지 중복 제거를 선택하여 기본 메시지 중복 제거를 활성화할 수 있습니다. 자세한 내용은 FIFO 주제에 대한 메시지 중복 제거를 참조하세요.

5. (선택 사항) 암호화 섹션을 확장하고 다음을 수행합니다. 자세한 내용은 저장된 데이터 암호화를 참조하세요.

   a. 암호화 활성을 선택합니다.

   b. 고객 마스터 키(CMK)를 지정합니다. 자세한 내용을 알아보려면 주요 용어를 참조하세요.

      각 CMK 유형에 대해 설명, 계정 및 CMK ARN이 표시됩니다.

      > **Important**
      >
      > 해당 CMK의 소유자가 아니거나 `kms:ListAliases` 및 `kms:DescribeKey` 권한이 없는 계정으로 로그인하는 경우, Amazon SNS 콘솔에서 해당 CMK에 대한 정보를 볼 수 없습니다.
      > CMK의 소유자에게 이 권한을 부여해 달라고 요청해야 합니다. 자세한 정보는 AWS Key Management Service 개발자 안내서의 AWS KMS API 권한: 작업 및 리소스 참조를 참조하세요.

      - Amazon SNS(기본값) alias/aws/sns에 대한 AWS 관리형 CMK가 기본적으로 선택됩니다.

        > **Note**
        >
        > 다음 사항에 유의하세요:
        >
        > - AWS Management Console 를 사용하여 주제에 대한 Amazon SNS용 AWS 관리형 CMK를 처음 지정하면가 Amazon SNS용 AWS 관리형 CMK를 AWS KMS 생성합니다.
        > - 또는 SSE가 활성화된 주제에 대해 `Publish` 작업을 처음 사용할 때가 Amazon SNS용 AWS 관리형 CMK를 AWS KMS 생성합니다.

      - 에서 사용자 지정 CMK를 사용하려면 AWS 계정고객 마스터 키(CMK) 필드를 선택한 다음 목록에서 사용자 지정 CMK를 선택합니다.

> **Note**
>
> 사용자 지정 CMK 생성에 대한 지침은 AWS Key Management Service 개발자 안내서의 키 생성을 참조하세요.

- AWS 계정 또는 다른 AWS 계정의 사용자 지정 CMK ARN을 사용하려면 고객 마스터 키(CMK) 필드에 입력합니다.

6. (선택 사항) 기본적으로 주제 소유자만 주제에 게시하거나 주제를 구독할 수 있습니다. 추가 액세스 권한을 구성하려면 액세스 정책 섹션을 확장합니다. 자세한 내용은 Amazon SNS의 Identity and Access Management 및 Amazon SNS 액세스 제어의 예제 사례를 참조하세요.

> **Note**
>
> 콘솔을 사용하여 주제를 생성하는 경우 기본 정책은 `aws:SourceOwner` 조건 키를 사용합니다. 이 키는 `aws:SourceAccount`와 비슷합니다.

7. (선택 사항) Amazon SNS가 실패한 메시지 전송을 재시도하는 방식을 구성하려면 전송 재시도 정책(HTTP/S) 섹션을 확장합니다. 자세한 내용은 Amazon SNS 메시지 전달 재시도를 참조하세요.
8. (선택 사항) Amazon SNS가 CloudWatch로의 메시지 전송을 로깅하는 방식을 구성하려면 전송 상태 로깅 섹션을 확장합니다. 자세한 내용은 Amazon SNS 메시지 전달 상태를 참조하세요.
9. (선택 사항) 메타데이터 태그를 주제에 추가하려면 태그 섹션을 확장하고, 키와 값(옵션)을 입력한 다음 태그 추가를 선택합니다. 자세한 내용은 Amazon SNS 주제 태그 지정을 참조하세요.
10. 주제 생성을 선택합니다.

    주제가 생성되고 ***MyTopic*** 페이지가 표시됩니다.

    주제의 이름, ARN, (선택 사항) 표시 이름 및 주제 소유자의 AWS 계정 ID가 세부 정보 섹션에 표시됩니다.
11. 다음 예와 같이 주제 ARN을 클립보드에 복사합니다.

```
arn:aws:sns:us-east-2:123456789012:MyTopic
```

이메일 주소에서 Amazon SNS 주제를 구독하려면

1. https://console.aws.amazon.com/sns/v3/home에서 Amazon SNS 콘솔을 엽니다.
2. 왼쪽의 탐색 창에서 구독을 선택합니다.

3. 구독 페이지에서 구독 생성을 선택합니다.
4. 구독 생성 페이지의 세부 정보 섹션에서 다음을 수행합니다.

   a. 주제 ARN에서 주제의 Amazon 리소스 이름(ARN)을 선택합니다.

   b. 프로토콜에서 엔드포인트 유형을 선택합니다. 사용 가능한 엔드포인트 유형은 다음과 같습니다.

      - HTTP/HTTPS
      - Email/Email-JSON
      - Amazon Data Firehose
      - Amazon SQS

      > **Note**
      > SNS FIFO 주제를 구독하려면 이 옵션을 선택합니다.

      - AWS Lambda
      - 플랫폼 애플리케이션 엔드포인트
      - SMS

   c. 엔드포인트에 이메일 주소 또는 Amazon SQS 대기열의 ARN과 같은 엔드포인트 값을 입력합니다.

   d. Firehose 엔드포인트만 해당: 구독 역할 ARN에서 Firehose 전송 스트림에 쓰기 위해 생성한 IAM 역할의 ARN을 지정합니다. 자세한 내용은 Firehose 전송 스트림에서 Amazon SNS 주제를 구독하기 위한 사전 조건을 참조하세요.

   e. (선택 사항) Firehose, Amazon SQS, HTTP/S 엔드포인트의 경우 원시 메시지 전송을 사용할 수도 있습니다. 자세한 내용은 Amazon SNS 원시 메시지 전송을 참조하세요.

   f. (선택 사항) 필터 정책을 구성하려면 구독 필터 정책 섹션을 확장합니다. 자세한 내용은 Amazon SNS 구독 필터 정책을 참조하세요.

   g. (선택 사항) 구독에 대한 배달 못한 편지 대기열을 구성하려면 리드라이브 정책(배달 못한 편지 대기열) 섹션을 확장합니다. 자세한 내용은 Amazon SQS DLQ(Dead Letter Queue)를 참조하세요.

   h. 구독 생성을 선택합니다.

   콘솔에서 구독을 만들고 구독의 세부 정보 페이지를 엽니다.

AWS SDKs 사용

AWS SDK를 사용하려면 자격 증명으로 구성해야 합니다. 자세한 정보는 AWS SDK 및 도구 참조 가이드의 공유 구성 및 자격 증명 파일을 참조하세요.

다음 코드 예시는 `CreateTopic`의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

특정 이름으로 주제를 생성합니다.

```
using System;
using System.Threading.Tasks;
using Amazon.SimpleNotificationService;
using Amazon.SimpleNotificationService.Model;

/// <summary>
/// This example shows how to use Amazon Simple Notification Service
/// (Amazon SNS) to add a new Amazon SNS topic.
/// </summary>
public class CreateSNSTopic
{
    public static async Task Main()
    {
        string topicName = "ExampleSNSTopic";

        IAmazonSimpleNotificationService client = new
AmazonSimpleNotificationServiceClient();

        var topicArn = await CreateSNSTopicAsync(client, topicName);
        Console.WriteLine($"New topic ARN: {topicArn}");
    }

    /// <summary>
    /// Creates a new SNS topic using the supplied topic name.
```

```
        /// </summary>
        /// <param name="client">The initialized SNS client object used to
        /// create the new topic.</param>
        /// <param name="topicName">A string representing the topic name.</param>
        /// <returns>The Amazon Resource Name (ARN) of the created topic.</
returns>
        public static async Task<string>
 CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
        {
            var request = new CreateTopicRequest
            {
                Name = topicName,
            };

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

이름과 특정 FIFO 및 중복 제거 속성을 사용하여 새 주제를 생성합니다.

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
    /// <param name="useFifoTopic">True to use a FIFO topic.</param>
    /// <param name="useContentBasedDeduplication">True to use content-based de-
duplication.</param>
    /// <returns>The ARN of the new topic.</returns>
    public async Task<string> CreateTopicWithName(string topicName, bool
 useFifoTopic, bool useContentBasedDeduplication)
    {
        var createTopicRequest = new CreateTopicRequest()
        {
            Name = topicName,
        };

        if (useFifoTopic)
        {
```

```
            // Update the name if it is not correct for a FIFO topic.
            if (!topicName.EndsWith(".fifo"))
            {
                createTopicRequest.Name = topicName + ".fifo";
            }

            // Add the attributes from the method parameters.
            createTopicRequest.Attributes = new Dictionary<string, string>
            {
                { "FifoTopic", "true" }
            };
            if (useContentBasedDeduplication)
            {
                createTopicRequest.Attributes.Add("ContentBasedDeduplication",
 "true");
            }
        }

        var createResponse = await
 _amazonSNSClient.CreateTopicAsync(createTopicRequest);
        return createResponse.TopicArn;
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 CreateTopic을 참조하세요.

C++

SDK for C++

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
//! Create an Amazon Simple Notification Service (Amazon SNS) topic.
/*!
  \param topicName: An Amazon SNS topic name.
  \param topicARNResult: String to return the Amazon Resource Name (ARN) for the
 topic.
  \param clientConfiguration: AWS client configuration.
```

```
  \return bool: Function succeeded.
 */
bool AwsDoc::SNS::createTopic(const Aws::String &topicName,
                              Aws::String &topicARNResult,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SNS::SNSClient snsClient(clientConfiguration);

    Aws::SNS::Model::CreateTopicRequest request;
    request.SetName(topicName);

    const Aws::SNS::Model::CreateTopicOutcome outcome =
 snsClient.CreateTopic(request);

    if (outcome.IsSuccess()) {
        topicARNResult = outcome.GetResult().GetTopicArn();
        std::cout << "Successfully created an Amazon SNS topic " << topicName
                  << " with topic ARN '" << topicARNResult
                  << "'." << std::endl;

    }
    else {
        std::cerr << "Error creating topic " << topicName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
        topicARNResult.clear();
    }

    return outcome.IsSuccess();
}
```

- API 세부 정보는 AWS SDK for C++ API 참조의 CreateTopic을 참조하세요.

CLI

AWS CLI

SNS 주제를 생성하려면

다음 `create-topic`예제에서는 `my-topic`이라는 SNS 주제를 생성합니다.

```
aws sns create-topic \
```

```
    --name my-topic
```

출력:

```
{
    "ResponseMetadata": {
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

자세한 내용은 AWS 명령줄 인터페이스 사용 설명서의 Amazon SQS 및 Amazon SNS에서 명령줄 인터페이스 사용을 참조하세요. AWS

- API 세부 정보는 AWS CLI 명령 참조의 CreateTopic을 참조하세요.

Go

SDK for Go V2

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/sns"
 "github.com/aws/aws-sdk-go-v2/service/sns/types"
)

// SnsActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type SnsActions struct {
```

```
 SnsClient *sns.Client
}



// CreateTopic creates an Amazon SNS topic with the specified name. You can
 optionally
// specify that the topic is created as a FIFO topic and whether it uses content-
based
// deduplication instead of ID-based deduplication.
func (actor SnsActions) CreateTopic(ctx context.Context, topicName string,
 isFifoTopic bool, contentBasedDeduplication bool) (string, error) {
 var topicArn string
 topicAttributes := map[string]string{}
 if isFifoTopic {
  topicAttributes["FifoTopic"] = "true"
 }
 if contentBasedDeduplication {
  topicAttributes["ContentBasedDeduplication"] = "true"
 }
 topic, err := actor.SnsClient.CreateTopic(ctx, &sns.CreateTopicInput{
  Name:       aws.String(topicName),
  Attributes: topicAttributes,
 })
 if err != nil {
  log.Printf("Couldn't create topic %v. Here's why: %v\n", topicName, err)
 } else {
  topicArn = *topic.TopicArn
 }

 return topicArn, err
}
```

- API 세부 정보는 AWS SDK for Go API 참조의 CreateTopic을 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sns.SnsClient;
import software.amazon.awssdk.services.sns.model.CreateTopicRequest;
import software.amazon.awssdk.services.sns.model.CreateTopicResponse;
import software.amazon.awssdk.services.sns.model.SnsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateTopic {
    public static void main(String[] args) {
        final String usage = """

                Usage:    <topicName>

                Where:
                   topicName - The name of the topic to create (for example,
 mytopic).

                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }
```

```
        String topicName = args[0];
        System.out.println("Creating a topic with name: " + topicName);
        SnsClient snsClient = SnsClient.builder()
                .region(Region.US_EAST_1)
                .build();

        String arnVal = createSNSTopic(snsClient, topicName);
        System.out.println("The topic ARN is" + arnVal);
        snsClient.close();
    }

    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

            result = snsClient.createTopic(request);
            return result.topicArn();

        } catch (SnsException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }
}
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 CreateTopic을 참조하세요.

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

별도의 모듈에서 클라이언트를 생성하고 내보냅니다.

```
import { SNSClient } from "@aws-sdk/client-sns";

// The AWS Region can be provided here using the `region` property. If you leave
 it blank
// the SDK will default to the region set in your AWS config.
export const snsClient = new SNSClient({});
```

SDK 및 클라이언트 모듈을 가져오고 API를 호출합니다.

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
import { snsClient } from "../libs/snsClient.js";

/**
 * @param {string} topicName - The name of the topic to create.
 */
export const createTopic = async (topicName = "TOPIC_NAME") => {
  const response = await snsClient.send(
    new CreateTopicCommand({ Name: topicName }),
  );
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '087b8ad2-4593-50c4-a496-d7e90b82cf3e',
  //     extendedRequestId: undefined,
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
  //   TopicArn: 'arn:aws:sns:us-east-1:xxxxxxxxxxxx:TOPIC_NAME'
  // }
  return response;
};
```

- 자세한 정보는 AWS SDK for JavaScript 개발자 안내서를 참조하십시오.
- API 세부 정보는 AWS SDK for JavaScript API 참조의 CreateTopic을 참조하세요.

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
suspend fun createSNSTopic(topicName: String): String {
    val request =
        CreateTopicRequest {
            name = topicName
        }

    SnsClient { region = "us-east-1" }.use { snsClient ->
        val result = snsClient.createTopic(request)
        return result.topicArn.toString()
    }
}
```

- API 세부 정보는 AWS SDK for Kotlin API 참조의 CreateTopic를 참조하세요.

PHP

SDK for PHP

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
require 'vendor/autoload.php';

use Aws\Exception\AwsException;
use Aws\Sns\SnsClient;
```

```
/**
 * Create a Simple Notification Service topics in your AWS account at the
 requested region.
 *
 * This code expects that you have AWS credentials set up per:
 * https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/
guide_credentials.html
 */

$SnSclient = new SnsClient([
    'profile' => 'default',
    'region' => 'us-east-1',
    'version' => '2010-03-31'
]);

$topicname = 'myTopic';

try {
    $result = $SnSclient->createTopic([
        'Name' => $topicname,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    // output error message if fails
    error_log($e->getMessage());
}
```

- 자세한 정보는 AWS SDK for PHP 개발자 안내서를 참조하세요.
- API 세부 정보는 AWS SDK for PHP API 참조의 CreateTopic을 참조하세요.

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""

    def __init__(self, sns_resource):
        """
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource


    def create_topic(self, name):
        """
        Creates a notification topic.

        :param name: The name of the topic to create.
        :return: The newly created topic.
        """
        try:
            topic = self.sns_resource.create_topic(Name=name)
            logger.info("Created topic %s with ARN %s.", name, topic.arn)
        except ClientError:
            logger.exception("Couldn't create topic %s.", name)
            raise
        else:
            return topic
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 CreateTopic를 참조하세요.

Ruby

SDK for Ruby

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
# This class demonstrates how to create an Amazon Simple Notification Service
 (SNS) topic.
class SNSTopicCreator
  # Initializes an SNS client.
  #
  # Utilizes the default AWS configuration for region and credentials.
  def initialize
    @sns_client = Aws::SNS::Client.new
  end

  # Attempts to create an SNS topic with the specified name.
  #
  # @param topic_name [String] The name of the SNS topic to create.
  # @return [Boolean] true if the topic was successfully created, false
 otherwise.
  def create_topic(topic_name)
    @sns_client.create_topic(name: topic_name)
    puts "The topic '#{topic_name}' was successfully created."
    true
  rescue Aws::SNS::Errors::ServiceError => e
    # Handles SNS service errors gracefully.
    puts "Error while creating the topic named '#{topic_name}': #{e.message}"
    false
  end
end

# Example usage:
if $PROGRAM_NAME == __FILE__
  topic_name = 'YourTopicName' # Replace with your topic name
  sns_topic_creator = SNSTopicCreator.new

  puts "Creating the topic '#{topic_name}'..."
  unless sns_topic_creator.create_topic(topic_name)
    puts 'The topic was not created. Stopping program.'
    exit 1
  end
end
```

- 자세한 정보는 AWS SDK for Ruby 개발자 안내서를 참조하세요.
- API 세부 정보는 AWS SDK for Ruby API 참조의 CreateTopic을 참조하세요.

Rust

SDK for Rust

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
async fn make_topic(client: &Client, topic_name: &str) -> Result<(), Error> {
    let resp = client.create_topic().name(topic_name).send().await?;

    println!(
        "Created topic with ARN: {}",
        resp.topic_arn().unwrap_or_default()
    );

    Ok(())
}
```

- API 세부 정보는 AWS SDK for Rust API 참조의 CreateTopic을 참조하세요.

SAP ABAP

SDK for SAP ABAP API

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    TRY.
        oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
 is returned for testing purposes. "
        MESSAGE 'SNS topic created' TYPE 'I'.
      CATCH /aws1/cx_snstopiclimitexcdex.
```

```
        MESSAGE 'Unable to create more topics. You have reached the maximum
number of topics allowed.' TYPE 'E'.
   ENDTRY.
```

- API에 대한 세부 정보는 SAP ABAP용AWS SDK API 참조의 CreateTopic을 참조하세요.

Swift

SDK for Swift

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import AWSSNS

        let config = try await SNSClient.SNSClientConfiguration(region: region)
        let snsClient = SNSClient(config: config)

        let output = try await snsClient.createTopic(
            input: CreateTopicInput(name: name)
        )

        guard let arn = output.topicArn else {
            print("No topic ARN returned by Amazon SNS.")
            return
        }
```

- API 세부 정보는 SDK for Swift API 참조의 CreateTopic을 참조하세요. AWS

> **Note**
>
> 다른 계정의 Amazon SNS 주제를 사용할 수도 있으나, 이 경우 주제에 대해 AWS Config에 액세스 권한을 부여하는 정책을 생성해야 할 수 있습니다. Amazon SNS 주제에 권한을 부여하는

방법에 대한 자세한 내용은 Amazon SNS 주제에 대한 권한 섹션을 참조한 후 3단계: IAM 역할 생성 섹션으로 이동하세요.

3단계: IAM 역할 생성

> **Important**
>
> (권장) AWS Config 서비스 연결 역할 사용
> AWS Config 서비스 연결 역할인를 사용하는 것이 좋습니다`AWSServiceRoleForConfig`. 서비스 연결 역할은 사전 정의되며가 다른를 호출하는 데 AWS Config 필요한 모든 권한을 포함합니다 AWS 서비스. AWS Config 서비스 연결 구성 레코더에는 서비스 연결 역할이 필요합니다.
> 자세한 내용은 AWS Config에 대한 서비스 연결 역할 사용을 참조하십시오.

IAM 콘솔 사용

IAM 콘솔을 사용하여 Amazon S3 버킷에 액세스하고, Amazon SNS 주제에 액세스하고, 지원되는 AWS 리소스에 대한 구성 세부 정보를 가져올 수 있는 AWS Config 권한을 부여하는 IAM 역할을 생성할 수 있습니다. 콘솔을 사용하여 IAM 역할을 생성하면 AWS Config 가 해당 역할에 필요한 권한을 자동으로 연결합니다.

> **Note**
>
> 가 사용하는 AWS 서비스 AWS Config (예: AWS Security Hub 또는 AWS Control Tower)를 사용했고 AWS Config 역할이 이미 생성된 경우 다른 AWS 서비스가 예상대로 계속 실행되도록 설정 시 사용하는 IAM 역할이 이미 생성된 AWS Config 역할과 동일한 최소 권한을 AWS Config 유지하는지 확인해야 합니다.
> 예를 들어 AWS Control Tower에가 Amazon S3 객체를 읽을 AWS Config 수 있도록 허용하는 IAM 역할이 있는 경우 설정 시 사용하는 IAM 역할 내에서 동일한 권한이 부여되도록 해야 합니다 AWS Config. 그렇지 않으면 AWS Control Tower의 작업을 방해할 수 있습니다.
> 의 IAM 역할에 대한 자세한 내용은 AWS Identity and Access Management를 AWS Config참조하세요.

AWS 서비스에 대한 역할을 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/iam/ IAM 콘솔을 엽니다.
2. IAM 콘솔의 탐색 창에서 역할을 선택하고 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 선택(Select trusted entity)에서 AWS 서비스(service)를 선택합니다.
4. Config - Customizable, AWS ConfigConfig - Organizations, Config 또는 Config - Conformance Packs 중에서 원하는 사용 사례를 선택합니다. 그리고 다음을 선택합니다.
5. 이름 지정, 검토 및 생성 페이지에서 역할에 대한 세부 정보를 검토한 후 역할 생성을 선택합니다.

AWS SDKs 사용

AWS SDK를 사용하려면 자격 증명으로 구성해야 합니다. 자세한 정보는 AWS SDK 및 도구 참조 가이드의 공유 구성 및 자격 증명 파일을 참조하세요.

다음 코드 예시는 `CreateRole`의 사용 방법을 보여 줍니다.

.NET

SDK for .NET

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role.</param>
    /// <param name="rolePolicyDocument">The name of the IAM policy document
    /// for the new role.</param>
    /// <returns>The Amazon Resource Name (ARN) of the role.</returns>
    public async Task<string> CreateRoleAsync(string roleName, string
rolePolicyDocument)
    {
        var request = new CreateRoleRequest
        {
            RoleName = roleName,
```

```
            AssumeRolePolicyDocument = rolePolicyDocument,
        };

        var response = await _IAMService.CreateRoleAsync(request);
        return response.Role.Arn;
    }
```

- API 세부 정보는 AWS SDK for .NET API 참조의 CreateRole을 참조하세요.

Bash

AWS CLI Bash 스크립트 사용

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_role
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
#       The ARN of the role.
#     And:
```

```
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) role."
    echo "  -n role_name   The name of the IAM role."
    echo "  -p policy_json -- The assume role policy document."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      p) policy_document="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
    usage
    return 1
  fi

  if [[ -z "$policy_document" ]]; then
    errecho "ERROR: You must provide a policy document with the -p parameter."
    usage
    return 1
```

```
  fi

  response=$(aws iam create-role \
    --role-name "$role_name" \
    --assume-role-policy-document "$policy_document" \
    --output text \
    --query Role.Arn)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- API 세부 정보는 AWS CLI 명령 참조의 CreateRole을 참조하세요.

C++

SDK for C++

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
bool AwsDoc::IAM::createIamRole(
        const Aws::String &roleName,
        const Aws::String &policy,
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::IAM::IAMClient client(clientConfig);
    Aws::IAM::Model::CreateRoleRequest request;

    request.SetRoleName(roleName);
```

```
    request.SetAssumeRolePolicyDocument(policy);

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- API 세부 정보는 AWS SDK for C++ API 참조의 CreateRole을 참조하세요.

CLI

AWS CLI

예제 1: IAM 역할 생성

다음 `create-role` 명령은 이름이 `Test-Role`인 역할을 생성하고 해당 역할에 신뢰 정책을 연결합니다.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

출력:

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
        "RoleName": "Test-Role",
        "Path": "/",
```

```
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

신뢰 정책은 Test-Role-Trust-Policy.json 파일에 JSON 문서로 정의됩니다. (파일 이름과 확장자는 중요하지 않습니다.) 신뢰 정책에서 보안 주체를 지정해야 합니다.

역할에 권한 정책을 연결하려면 `put-role-policy` 명령을 사용합니다.

자세한 내용은 AWS IAM 사용 설명서의 IAM 역할 생성을 참조하세요.

예제 2: 지정된 최대 세션 시간을 포함한 IAM 역할 생성

다음 `create-role` 명령은 이름이 `Test-Role`인 역할을 생성하고 최대 세션 지속 시간을 7,200초(2시간)로 설정합니다.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --max-session-duration 7200
```

출력:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
```

```
    }
}
```

자세한 내용은 AWS IAM 사용 설명서의 역할 최대 세션 기간(AWS API) 수정을 참조하세요.

예제 3: 태그가 포함된 IAM 역할 생성

다음 명령은 태그가 포함된 IAM 역할 `Test-Role`을 생성합니다. 이 예제에서는 다음 JSON 형식의 태그(`'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`)에 `--tags` 파라미터 플래그를 사용합니다. 또는 `--tags` 플래그를 짧은 형식의 태그(`'Key=Department,Value=Accounting Key=Location,Value=Seattle'`)에 사용할 수도 있습니다.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

출력:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Tags": [
```

```
            {
                "Key": "Department",
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
        ]
    }
}
```

자세한 내용은 AWS IAM 사용 설명서의 IAM 역할 태그 지정을 참조하세요.

- API 세부 정보는 AWS CLI 명령 참조의 CreateRole을 참조하세요.

Go

SDK for Go V2

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/iam"
 "github.com/aws/aws-sdk-go-v2/service/iam/types"
)

// RoleWrapper encapsulates AWS Identity and Access Management (IAM) role actions
// used in the examples.
// It contains an IAM service client that is used to perform role actions.
type RoleWrapper struct {
 IamClient *iam.Client
```

```
}



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
func (wrapper RoleWrapper) CreateRole(ctx context.Context, roleName string,
 trustedUserArn string) (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version: "2012-10-17",
  Statement: []PolicyStatement{{
   Effect:    "Allow",
   Principal: map[string]string{"AWS": trustedUserArn},
   Action:    []string{"sts:AssumeRole"},
  }},
 }
 policyBytes, err := json.Marshal(trustPolicy)
 if err != nil {
  log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
 trustedUserArn, err)
  return nil, err
 }
 result, err := wrapper.IamClient.CreateRole(ctx, &iam.CreateRoleInput{
  AssumeRolePolicyDocument: aws.String(string(policyBytes)),
  RoleName:                 aws.String(roleName),
 })
 if err != nil {
  log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
 } else {
  role = result.Role
 }
 return role, err
}
```

- API 세부 정보는 AWS SDK for Go API 참조의 CreateRole을 참조하세요.

Java

SDK for Java 2.x

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import org.json.simple.JSONObject;
import org.json.simple.parser.JSONParser;
import software.amazon.awssdk.services.iam.model.CreateRoleRequest;
import software.amazon.awssdk.services.iam.model.CreateRoleResponse;
import software.amazon.awssdk.services.iam.model.IamException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

/*
*   This example requires a trust policy document. For more information, see:
*   https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-
roles/
*
*
*  In addition, set up your development environment, including your credentials.
*
*  For information, see this documentation topic:
*
*  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
                Usage:
                    <rolename> <fileLocation>\s

                Where:
                    rolename - The name of the role to create.\s
```

```
                    fileLocation - The location of the JSON document that
represents the trust policy.\s
                """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String rolename = args[0];
        String fileLocation = args[1];
        Region region = Region.AWS_GLOBAL;
        IamClient iam = IamClient.builder()
                .region(region)
                .build();

        String result = createIAMRole(iam, rolename, fileLocation);
        System.out.println("Successfully created user: " + result);
        iam.close();
    }

    public static String createIAMRole(IamClient iam, String rolename, String
fileLocation) throws Exception {
        try {
            JSONObject jsonObject = (JSONObject)
readJsonSimpleDemo(fileLocation);
            CreateRoleRequest request = CreateRoleRequest.builder()
                    .roleName(rolename)
                    .assumeRolePolicyDocument(jsonObject.toJSONString())
                    .description("Created using the AWS SDK for Java")
                    .build();

            CreateRoleResponse response = iam.createRole(request);
            System.out.println("The ARN of the role is " +
response.role().arn());

        } catch (IamException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }

    public static Object readJsonSimpleDemo(String filename) throws Exception {
```

```
        FileReader reader = new FileReader(filename);
        JSONParser jsonParser = new JSONParser();
        return jsonParser.parse(reader);
    }
}
```

- API 세부 정보는 AWS SDK for Java 2.x API 참조의 CreateRole을 참조하세요.

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

역할을 생성합니다.

```
import { CreateRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
        },
      ],
```

```
    }),
    RoleName: roleName,
  });

  return client.send(command);
};
```

- API 세부 정보는 AWS SDK for JavaScript API 참조의 CreateRole을 참조하세요.

PHP

SDK for PHP

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
$uuid = uniqid();
$service = new IAMService();

$assumeRolePolicyDocument = "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Principal\": {\"AWS\": \"{$user['Arn']}\"},
                    \"Action\": \"sts:AssumeRole\"
                }]
            }";
$assumeRoleRole = $service->createRole("iam_demo_role_$uuid",
 $assumeRolePolicyDocument);
echo "Created role: {$assumeRoleRole['RoleName']}\n";

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
     * @return array
     * @throws AwsException
     */
    public function createRole(string $roleName, string $rolePolicyDocument)
```

```
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
            ]);
        });
        return $result['Role'];
    }
```

- API 세부 정보는 AWS SDK for PHP API 참조의 CreateRole을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제는 **MyNewRole**이라는 새 역할을 생성하고 여기에 **NewRoleTrustPolicy.json** 파일에 있는 정책을 연결합니다. JSON 정책 파일을 성공적으로 처리하려면 **-Raw** 스위치 파라미터를 사용해야 합니다. 출력에 표시된 정책 문서는 URL로 인코딩됩니다. 이 예제에서는 **UrlDecode** .NET 메서드를 사용하여 디코딩됩니다.

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

출력:

```
Arn                       : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                           %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
```

```
                              %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                              %20%5D%0D%0A%7D
CreateDate                  : 4/15/2015 11:04:23 AM
Path                        : /
RoleId                      : V5PAJI2KPN4EAEXAMPLE1
RoleName                    : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조(V4)의 CreateRole을 참조하세요.

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
def create_role(role_name, allowed_services):
    """
    Creates a role that lets a list of specified services assume the role.

    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
```

```
    :return: The newly created role.
    """
    trust_policy = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {"Service": service},
                "Action": "sts:AssumeRole",
            }
            for service in allowed_services
        ],
    }

    try:
        role = iam.create_role(
            RoleName=role_name, AssumeRolePolicyDocument=json.dumps(trust_policy)
        )
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
    else:
        return role
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 CreateRole를 참조하세요.

Ruby

SDK for Ruby

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
# Creates a role and attaches policies to it.
#
```

```
  # @param role_name [String] The name of the role.
  # @param assume_role_policy_document [Hash] The trust relationship policy
 document.
  # @param policy_arns [Array<String>] The ARNs of the policies to attach.
  # @return [String, nil] The ARN of the new role if successful, or nil if an
 error occurred.
  def create_role(role_name, assume_role_policy_document, policy_arns)
    response = @iam_client.create_role(
      role_name: role_name,
      assume_role_policy_document: assume_role_policy_document.to_json
    )
    role_arn = response.role.arn

    policy_arns.each do |policy_arn|
      @iam_client.attach_role_policy(
        role_name: role_name,
        policy_arn: policy_arn
      )
    end

    role_arn
  rescue Aws::IAM::Errors::ServiceError => e
    @logger.error("Error creating role: #{e.message}")
    nil
  end
```

- API 세부 정보는 AWS SDK for Ruby API 참조의 CreateRole을 참조하세요.

Rust

SDK for Rust

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
```

```
    role_policy_document: &str,
) -> Result<Role, iamError> {
    let response: CreateRoleOutput = loop {
        if let Ok(response) = client
            .create_role()
            .role_name(role_name)
            .assume_role_policy_document(role_policy_document)
            .send()
            .await
        {
            break response;
        }
    };

    Ok(response.role.unwrap())
}
```

- API 세부 정보는 AWS SDK for Rust API 참조의 CreateRole을 참조하세요.

Swift

SDK for Swift

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
import AWSIAM
import AWSS3


    public func createRole(name: String, policyDocument: String) async throws ->
 String {
        let input = CreateRoleInput(
            assumeRolePolicyDocument: policyDocument,
            roleName: name
        )
        do {
            let output = try await client.createRole(input: input)
```

```
            guard let role = output.role else {
                throw ServiceHandlerError.noSuchRole
            }
            guard let id = role.roleId else {
                throw ServiceHandlerError.noSuchRole
            }
            return id
        } catch {
            print("ERROR: createRole:", dump(error))
            throw error
        }
    }
```

- API 세부 정보는 AWS SDK for Swift API 참조의 CreateRole을 참조하세요.

를 사용하여 고객 관리형 구성 레코더 AWS Config 로 시작 AWS CLI

고객 관리형 구성 레코더를 생성 AWS Config 하여 시작할 수 있습니다. 를 사용하여 고객 관리형 구성 레코더를 생성하려면 AWS CLI, `put-configuration-recorder` `put-delivery-channel`및 명령을 사용합니다`start-configuration-recorder`.

- 이 `put-configuration-recorder` 명령은 고객 관리형 구성 레코더를 생성합니다.
- 이 `put-delivery-channel` 명령은가 S3 버킷 및 SNS 주제에 구성 정보를 AWS Config 전송하는 전송 채널을 생성합니다.
- 는 고객 관리형 구성 레코더를 `start-configuration-recorder` 시작합니다. 고객 관리형 구성 레코더는 지정한 리소스 유형에 대한 구성 변경 사항 기록을 시작합니다.

주제

- 고려 사항
- 1단계: put-configuration-recorder 실행
- 2단계: put-delivery-channel 명령 실행
- 3단계: start-configuration-recorder 명령 실행

고려 사항

S3 버킷, SNS 주제 및 IAM 역할이 필요합니다.

고객 관리형 구성 레코더를 생성하려면 S3 버킷, SNS 주제 및 정책이 사전 조건으로 연결된 IAM 역할을 생성해야 합니다. 에 대한 사전 조건을 설정하려면 사전 조건을 AWS Config참조하세요. https://docs.aws.amazon.com/config/latest/developerguide/gs-cli-prereq.html

리전별 계정당 고객 관리형 구성 레코더 1개

각에 대해 각각 하나의 고객 관리형 구성 레코더만 가질 수 AWS 계정 있습니다 AWS 리전.

리전당 계정당 하나의 전송 채널

각에 대해 하나의 전송 채널 리전만 가질 수 AWS 계정 있습니다 AWS 리전.

정책 및 규정 준수 결과

에서 관리되는 IAM 정책 및 기타 정책은에 리소스에 대한 구성 변경을 기록할 권한이 있는지 여부에 AWS Config 영향을 미칠 수 있습니다. AWS Organizations 또한 규칙은 리소스의 구성을 직접 평가하며, 규칙은 평가를 실행할 때 이러한 정책을 고려하지 않습니다. 적용 중인 정책이 사용 의도와 일치하는지 확인합니다 AWS Config.

1단계: put-configuration-recorder 실행

`put-configuration-recorder` 명령을 사용하여 고객 관리형 구성 레코더를 생성합니다.

이 명령은 `--configuration-recorder` 및 `---recording-group` 필드를 사용합니다.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

`configuration-recorder` 필드

`configurationRecorder.json` 파일이 `name`, `roleArn` 및 구성 레코더(`recordingMode`)의 기본 기록 빈도를 지정합니다. 또한이 필드를 사용하여 특정 리소스 유형에 대한 기록 빈도를 재정의할 수 있습니다.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
```

```
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in the
 override ]
        }
    ]
  }
}
```

recording-group 필드

recordingGroup.json 파일은 기록되는 리소스 유형을 지정합니다.

```
{
    "allSupported": boolean,
    "exclusionByResourceTypes": {
        "resourceTypes": [ Comma-separated list of resource types to exclude ]
    },
    "includeGlobalResourceTypes": boolean,
    "recordingStrategy": {
        "useOnly": "Recording strategy for the configuration recorder"
    },
    "resourceTypes": [ Comma-separated list of resource types to include]
}
```

이러한 필드에 대한 자세한 내용은 AWS CLI 명령 참조put-configuration-recorder의 섹션을 참조하세요.

2단계: put-delivery-channel 명령 실행

put-delivery-channel 명령을 사용하여 전송 채널을 생성합니다.

이 명령은 --delivery-channel 필드를 사용합니다.

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

delivery-channel 필드

deliveryChannel.json 파일은 다음을 지정합니다.

- 전송 채널name의 입니다.

- 가 구성 스냅샷을 AWS Config 전송하는 `s3BucketName` 입니다.
- 가 알림을 AWS Config 보내는 `snsTopicARN`
- `configSnapshotDeliveryProperties`가 구성 스냅샷을 AWS Config 전송하는 빈도와 정기 규칙에 대한 평가를 호출하는 빈도를 설정하는 입니다.

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

이러한 필드에 대한 자세한 내용은 AWS CLI 명령 참조`put-delivery-channel`의 섹션을 참조하세요.

3단계: start-configuration-recorder 명령 실행

`start-configuration-recorder` 명령을 사용하여 시작합니다 AWS Config.

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

이러한 필드에 대한 자세한 내용은 AWS CLI 명령 참조`start-configuration-recorder`의 섹션을 참조하세요.

이 로 성공적으로 시작 AWS Config 되었는지 확인 AWS CLI

시작한 후 AWS CLI 명령을 사용하여가 실행 AWS Config 중이고 구성 레코더와 전송 채널을 생성 AWS Config 했는지 확인할 AWS Config수 있습니다. AWS Config 가 구성을 기록하고 전송 채널로 전송하기 시작했음을 확인할 수도 있습니다.

주제

- 1단계: 전송 채널이 생성되었는지 확인
- 2단계: 구성 레코더가 생성되었는지 확인
- 3단계: AWS Config 가 레코딩을 시작했는지 확인

1단계: 전송 채널이 생성되었는지 확인

describe-delivery-channels 명령을 사용하여 Amazon S3 버킷과 Amazon SNS 주제가 구성되었는지 확인합니다.

`--delivery-channel-names` 필드를 사용하여 전송 채널 목록을 지정할 수 있습니다. 전송 채널을 지정하지 않으면이 명령은 계정과 연결된 모든 전송 채널의 세부 정보를 반환합니다.

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
            "name": "my-delivery-channel",
            "s3BucketName": "my-config-bucket"
        }
    ]
}
```

2단계: 구성 레코더가 생성되었는지 확인

describe-configuration-recorders 명령을 사용하여 구성 레코더가 생성되었는지 확인합니다.

`arn` 및 `configuration-recorder-names` 필드를 사용하여 구성 레코더 목록을 지정할 수 있습니다. 구성 레코더가 지정되지 않은 경우이 명령은 계정과 연결된 모든 구성 레코더의 세부 정보를 반환합니다.

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

3단계: AWS Config 가 레코딩을 시작했는지 확인

describe-configuration-recorder-status 명령을 사용하여 구성 레코더가 범위에서 리소스 유형을 성공적으로 기록하고 있는지 확인합니다.

arn 및 configuration-recorder-names 필드를 사용하여 구성 레코더 목록을 지정할 수 있습니다. 구성 레코더가 지정되지 않은 경우이 명령은 계정과 연결된 모든 구성 레코더의 세부 정보를 반환합니다.

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

recording 필드의 true 값은 구성 레코더가 구성을 기록하기 시작했음을 확인합니다. AWS Config는 시간을 UTC로 기록합니다. 출력은 Unix 타임스탬프로 표시됩니다.

AWS SDK AWS Config 에서 사용

AWS 소프트웨어 개발 키트(SDKs)는 널리 사용되는 많은 프로그래밍 언어에 사용할 수 있습니다. 각 SDK는 개발자가 선호하는 언어로 애플리케이션을 쉽게 구축할 수 있도록 하는 API, 코드 예시 및 설명서를 제공합니다.

SDK 설명서	코드 예제
AWS SDK for C++	AWS SDK for C++ 코드 예제
AWS CLI	AWS CLI 코드 예제
AWS SDK for Go	AWS SDK for Go 코드 예제
AWS SDK for Java	AWS SDK for Java 코드 예제
AWS SDK for JavaScript	AWS SDK for JavaScript 코드 예제

SDK 설명서	코드 예제
AWS SDK for Kotlin	AWS SDK for Kotlin 코드 예제
AWS SDK for .NET	AWS SDK for .NET 코드 예제
AWS SDK for PHP	AWS SDK for PHP 코드 예제
AWS Tools for PowerShell	Tools for PowerShell 코드 예시
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 코드 예제
AWS SDK for Ruby	AWS SDK for Ruby 코드 예제
AWS SDK for Rust	AWS SDK for Rust 코드 예제
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP 코드 예제
AWS SDK for Swift	AWS SDK for Swift 코드 예제

가용성 예제

필요한 예제를 찾을 수 없습니까? 이 페이지 하단의 피드백 제공 링크를 사용하여 코드 예시를 요청하세요.

구성 레코더 작업

구성 레코더는 범위 내 리소스 유형에 대한 구성 변경 사항을 구성 항목(CIs)으로 저장합니다.

구성 레코더에는 두 가지 유형이 있습니다.

유형	설명
고객 관리형 구성 레코더	관리한 구성 레코더입니다. 범위의 리소스 유형은 사용자가 설정합니다. 기본적으로 고객 관리형 구성 레코더는 AWS 리전 AWS Config 가 실행되는에서 지원되는 모든 리소스를 기록합니다.
서비스 연결 구성 레코더	특정에 연결된 구성 레코더입니다 AWS 서비스. 범위의 리소스 유형은 연결된 서비스에 의해 설정됩니다.

주제

- 고객 관리형 구성 레코더에 대한 고려 사항
- 서비스 연결 구성 레코더에 대한 고려 사항
- 구성 레코더에 대한 드리프트 감지
- 고객 관리형 구성 레코더 시작
- 고객 관리형 구성 레코더 중지
- 고객 관리형 구성 레코더의 레코딩 빈도 변경
- 고객 관리형 구성 레코더 이름 바꾸기
- 구성 레코더 보기
- 구성 레코더 삭제

고객 관리형 구성 레코더에 대한 고려 사항

리전별 계정당 고객 관리형 구성 레코더 1개

각에 대해 하나의 고객 관리형 구성 레코더만 가질 수 AWS 계정 있습니다 AWS 리전.

기본값은 글로벌 IAM 리소스 유형을 제외한 지원되는 모든 리소스 유형을 기록하는 것입니다.

고객 관리형 구성 레코더의 기본값은 , `AWS::IAM::Group`, `AWS::IAM::Policy` `AWS::IAM::Role`및 글로벌 IAM 리소스 유형을 제외하고 지원되는 모든 리소스 유형을 기록하는 것입니다. 기록에서 포함하거나 제외할 리소스 유형을 지정할 `AWS::IAM::User` 수 있습니다.

자세한 내용은 를 사용하여 AWS 리소스 기록 AWS Config 단원을 참조하십시오.

고객 관리형 구성 레코더 사용에 대한 서비스 사용 요금이 청구됩니다.

가 고객 관리형 구성 레코더로 구성 기록을 AWS Config 시작하면 서비스 사용 요금이 부과됩니다.

요금 정보는 AWS Config 요금을 참조하세요.

AWS Systems Manager 를 사용하여 조직 전체에서 고객 관리형 구성 레코더 생성

AWS Systems Manager 빠른 설정을 사용하여 여러 조직 단위(OUs)에서 고객 관리형 구성 레코더를 생성하고 AWS 모범 사례를 AWS 리전 사용할 수 있습니다.

자세한 내용은 Systems Manager 사용 설명서의 빠른 설정을 사용하여 AWS Config 구성 레코더 생성을 참조하세요.

> **Important**
>
> 정책 및 규정 준수 결과
> 에서 관리되는 IAM 정책 및 기타 정책은 AWS Config 에 리소스에 대한 구성 변경을 기록할 권한이 있는지 여부에 영향을 미칠 수 있습니다. AWS Organizations 또한 규칙은 리소스의 구성을 직접 평가하며, 규칙은 평가를 실행할 때 이러한 정책을 고려하지 않습니다. 적용 중인 정책이 사용 의도와 일치하는지 확인합니다 AWS Config.
> 구성 레코더가 꺼진 경우 삭제된 리소스에 대한 오래된 평가 결과가 지속될 수 있습니다.
> 고객 관리형 구성 레코더가 꺼져 있으면 삭제를 포함하여 지정한 리소스의 구성 변경을 추적하는 AWS Config Config의 기능이 비활성화됩니다. 즉, 기록이 켜져 있지 않으면가 삭제 이벤트를 캡처 AWS Config 할 수 없으므로 고객 관리형 구성 레코더가 꺼져 있을 때 삭제되는 리소스에 대한 오래된 평가 결과가 표시될 수 있습니다.

서비스 연결 구성 레코더에 대한 고려 사항

AWS Config 서비스 연결 역할을 사용해야 합니다.

AWS Config 서비스 연결 구성 레코더에는 서비스 연결 역할이 필요합니다.

자세한 내용은 AWS Config에 대한 서비스 연결 역할 사용을 참조하십시오.

서비스 연결 구성 레코더는 항상 기록됩니다.

서비스 연결 구성 레코더에 대한 레코딩을 중지하거나 시작할 수 없습니다. 기록을 중지하려면 서비스 연결 구성 레코더를 삭제해야 합니다.

자세한 내용은 구성 레코더 삭제를 참조하세요.

기록 범위에 따라 구성 항목의 수신 여부가 결정됩니다.

기록 범위는 구성 레코더에 연결된 서비스에 의해 설정되며 전송 채널에서 구성 항목(CIs)을 수신할지 여부를 결정합니다. 기록 범위가 내부인 경우 전송 채널에서 CIs를 수신하지 않습니다.

기록 범위에 따라 서비스 요금이 부과되는지 여부가 결정됩니다.

기록 범위는 구성 레코더에 연결된 서비스에 의해 설정되며 범위 내 구성 항목(CIs 무료로 기록되는지 (내부) 아니면 청구서 비용(PAID)에 영향을 미치는지(PAID)를 결정합니다.

지원되는 서비스

서비스 연결 구성 레코더는 다음 서비스에서 지원됩니다.

AWS service	서비스 보안 주체	와 함께를 사용할 때의 이점 AWS Config	자세히 알아보기
Amazon CloudWatch	`observabilityadmin.amazonaws.com`	Amazon CloudWatch Observability Admin을 사용하여 AWS 조직 또는 계정의 CloudWatch에서 원격 측정 구성 상태를 검색하고 이해할 수 있습니다.	자세한 내용은 CloudWatch 사용 설명서의 CloudWatch 원격 측정 구성 감사를 참조하세요. CloudWatch

구성 레코더에 대한 드리프트 감지

`AWS::Config::ConfigurationRecorder` 리소스 유형은 구성 레코더의 상태에 대한 모든 변경 사항을 추적하는 구성 레코더의 구성 항목(CI)입니다. 이 CI를 사용하여 구성 레코더의 상태가 이전 상태와 다른지, 즉 드리프트되었는지 확인할 수 있습니다.

예를 들어 이 CI는 AWS Config 가 추적하도록 설정한 리소스 유형에 대한 업데이트가 있는지, 구성 레코더를 중지 또는 시작했는지, 구성 레코더를 삭제 또는 제거했는지 추적합니다. 드리프트된 구성 레코더는 의도한 리소스 유형의 변경 사항을 정확하게 감지하지 못한다는 것을 나타냅니다. 구성 레코더가 드리프트된 경우 이로 인해 거짓 부정 또는 거짓 긍정 규정 준수 결과가 나올 수 있습니다.

`AWS::Config::ConfigurationRecorder` 리소스 유형은의 시스템 리소스 유형이며
이 리소스 유형의 AWS Config 기록은 지원되는 모든 리전에서 기본적으로 활성화됩니다.
`AWS::Config::ConfigurationRecorder` 리소스 유형 기록에는 추가 요금이 부과되지 않습니다.

고객 관리형 구성 레코더 시작

AWS Config 콘솔을 사용하거나 고객 관리형 구성 레코더를 AWS CLI 시작할 수 있습니다.

To start the customer managed configuration recorder (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 고객 관리형 레코더 탭에서 레코딩 시작을 선택합니다. 메시지가 표시되면 확인을 선택합니다.

To start the customer managed configuration recorder (CLI)

`start-configuration-recorder` 명령을 사용합니다.

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

고객 관리형 구성 레코더 중지

> **Note**
>
> 서비스 연결 구성 레코더는 항상 기록됩니다.

서비스 연결 구성 레코더는 항상 기록되므로 서비스 연결 구성 레코더를 중지할 수 없습니다. 기록을 중지하려면 서비스 연결 구성 레코더를 삭제해야 합니다. 자세한 내용은 구성 레코더 삭제를 참조하세요.

AWS Config 콘솔을 사용하거나 고객 관리형 구성 레코더를 AWS CLI 중지할 수 있습니다.

To stop the customer managed configuration recorder (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 고객 관리형 레코더 탭에서 레코딩 중지를 선택합니다. 메시지가 표시되면 확인을 선택합니다.

To stop the customer managed configuration recorder (CLI)

`stop-configuration-recorder` 명령을 사용합니다.

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

고객 관리형 구성 레코더의 레코딩 빈도 변경

AWS Config 는 연속 기록 및 일일 기록을 지원합니다.

- 연속 기록을 사용하면 변경이 발생할 때마다 구성 변경을 지속적으로 기록할 수 있습니다.
- 일별 기록을 사용하면 기록된 이전 CI와 다른 경우에만 지난 24시간 동안 리소스의 최신 상태를 나타내는 구성 항목(CI)을 수신할 수 있습니다. 자세한 내용은 기록 빈도를 참조하세요.

AWS Config 콘솔을 사용하거나 녹음 빈도를 AWS CLI 변경할 수 있습니다.

To change the recording frequency for the customer managed configuration recorder (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.

3. 고객 관리형 레코더 탭에서 레코딩 시작을 선택합니다.
4. 기록 방법 관리형 레코더에서 사용자 지정 가능한 재정의가 있는 모든 리소스 유형을 선택합니다.
5. 기본 설정에서 기록 빈도를 선택합니다.
6. 저장을 선택합니다.

To change the recording frequency (CLI)

put-configuration-recorder 명령을 사용하여 구성 레코더의 기록 빈도를 변경합니다.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json
```

configurationRecorder.json 파일이 name, roleArn 및 구성 레코더(recordingMode)의 기본 기록 빈도를 지정합니다. 이 필드를 사용하여 특정 리소스 유형의 기록 빈도를 재정의할 수도 있습니다.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
  }
}
```

put-configuration-recorder는 파라미터에 대해 다음 필드를 사용합니다.

- name - 구성 레코더의 이름입니다. AWS Config 이 구성 레코더를 생성할 때 '기본값' 이름을 자동으로 할당합니다.
- roleARN - 구성 레코더에서 수임 AWS Config 하고 사용하는 IAM 역할의 Amazon 리소스 이름(ARN)입니다.

- `recordingMode` -가 구성 변경을 기록하는 데 AWS Config 사용하는 기본 기록 빈도를 지정합니다.는 연속 기록 및 일별 기록을 AWS Config 지원합니다. 지속적인 기록을 사용하면 변경이 발생할 때마다 지속적으로 구성 변경 사항을 기록할 수 있습니다. 일일 기록을 사용하면 이전에 기록된 CI와 다른 경우에만 지난 24시간 동안의 리소스 최신 상태를 나타내는 구성 항목(CI)을 받을 수 있습니다.
  - `recordingFrequency` -가 구성 변경을 기록하는 데 AWS Config 사용하는 기본 기록 빈도입니다.

    > **Note**
    >
    > AWS Firewall Manager 는 리소스를 모니터링하기 위해 지속적인 레코딩에 의존합니다. Firewall Manager를 사용하는 경우 기록 빈도를 계속으로 설정하는 것이 좋습니다.

  - `recordingModeOverrides` - 이 필드를 사용하여 기록 모드에 대한 재정의를 지정할 수 있습니다. `recordingModeOverride` 객체 배열입니다. `recordingModeOverrides` 배열의 각 `recordingModeOverride` 객체는 세 개의 필드로 구성됩니다.
    - `description` - 재정의에 제공하는 설명입니다.
    - `recordingFrequency` - 재정의에 지정된 모든 리소스 유형에 적용되는 기록 빈도입니다.
    - `resourceTypes` - 재정의를 포함하는 리소스 유형을 지정하는 쉼표로 구분된 목록 AWS Config 입니다.

> **Note**
>
> 필수 및 선택 필드
>
> put-configuration-recorder에 대한 `recordingMode` 필드는 선택 사항입니다. 기본적으로 구성 레코더의 기록 빈도는 지속적인 기록으로 설정됩니다.

> **Note**
>
> Limits
>
> 다음과 같은 리소스 유형에는 일일 기록이 지원되지 않습니다.
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

현재 및 향후에 지원되는 모든 리소스 유형 기록(ALL_SUPPORTED_RESOURCE_TYPES) 기록 전략의 경우 이러한 리소스 유형이 지속적인 기록으로 설정됩니다.

고객 관리형 구성 레코더 이름 바꾸기

AWS CLI 를 사용하여 고객 관리형 구성 레코더의 이름을 변경해야 합니다. 고객 관리형 구성 레코더의 이름을 변경하려면 이름을 삭제하고 지정된 이름으로 새 구성 레코더를 생성해야 합니다.

를 사용하여 고객 관리형 구성 레코더 이름 바꾸기 AWS CLI

1. describe-configuration-recorders 명령을 사용하여 현재 고객 관리형 구성 레코더의 이름을 조회합니다.

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

2. delete-configuration-recorder 명령을 사용하여 고객 관리형 현재 구성 레코더를 삭제합니다.

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

3. put-configuration-recorder 명령을 사용하여 새 이름으로 고객 관리형 구성 레코더를 생성합니다.

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. 다음 start-configuration-recorder 명령을 사용하여 기록을 재개합니다.

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

구성 레코더 보기

AWS Config 콘솔을 사용하거나 구성 레코더에 대한 세부 정보를 AWS CLI 볼 수 있습니다.

To view your configuration recorders (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 고객 관리형 구성 레코더의 경우 고객 관리형 레코더 탭에서 세부 정보를 볼 수 있습니다.
4. 서비스 연결 구성 레코더의 경우 서비스 연결 레코더 탭에서 서비스 연결 구성 레코더를 선택한 다음 보기를 선택합니다.

To view your configuration recorders (CLI)

describe-configuration-recorders 명령을 사용하여 구성 레코더에 대한 세부 정보를 봅니다.

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

describe-configuration-recorder-status 명령을 사용하여 구성 레코더의 현재 상태를 확인합니다.

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
```

```
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

두 명령 모두 `arn` 및 `configuration-recorder-names` 필드를 사용하여 구성 레코더 목록을 지정할 수 있습니다. 서비스 연결 구성 레코더의 경우 `service-principal` 필드를 사용하여 구성 레코더를 지정할 수 있습니다.

구성 레코더가 지정되지 않은 경우이 명령은 계정과 연결된 모든 구성 레코더의 세부 정보를 반환합니다.

구성 레코더 삭제

고객 관리형 구성 레코더를 삭제 AWS CLI 하려면를 사용해야 합니다. AWS Config 콘솔 또는 AWS CLI 를 사용하여 서비스 연결 구성 레코더를 삭제할 수 있습니다.

To delete the customer managed configuration recorder (CLI)

`delete-configuration-recorder` 명령을 사용합니다.

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

To delete a service-linked configuration recorder (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 서비스 연결 레코더 탭의 서비스 연결 레코더 탭에서 서비스 연결 구성 레코더를 선택한 다음 삭제를 선택합니다. 확인 메시지가 나타나면 삭제를 선택합니다.

To delete a service-linked configuration recorder (CLI)

`delete-service-linked-configuration-recorder` 명령을 사용합니다.

이 명령은 `--service-principal` 필드를 사용합니다.

```
$ aws configservice delete-service-linked-configuration-recorder --service-principal
 "The service principal of the AWS ### for the service-linked configuration recorder
 that you want to delete"
```

전송 채널 작업

는 AWS 리소스에 발생하는 변경 사항을 AWS Config 지속적으로 기록하므로 전송 채널을 통해 알림 및 업데이트된 구성 상태를 전송합니다. 전송 채널을 관리하여가 구성 업데이트를 AWS Config 전송하는 위치를 제어할 수 있습니다.

주제

- 고려 사항
- 용어
- 구성 항목의 구성 요소
- 전송 채널 보기
- 전송 채널 업데이트
- 전송 채널의 이름 바꾸기
- 구성 스냅샷을 Amazon S3 버킷에 전송
- 전송 상태 확인
- Amazon S3 버킷의 구성 스냅샷 확인
- 의 구성 스냅샷 예제 AWS Config
- 가 Amazon SNS 주제로 AWS Config 보내는 알림

고려 사항

리전당 계정당 전송 채널 1개

AWS 리전당 리전당 하나의 전송 채널만 가질 수 AWS 계정있으며, 전송 채널을 사용해야 합니다 AWS Config.

크기 초과 구성 항목 알림에는 간략한 요약이 포함됩니다.

가 리소스에 대한 구성 변경을 AWS Config 감지하고 알림이 Amazon SNS에서 허용하는 최대 크기를 초과하는 경우 알림에는 구성 항목에 대한 간략한 요약이 포함됩니다. `s3BucketLocation` 필드에 지정된 Amazon S3 버킷 위치에서 전체 알림을 볼 수 있습니다. 자세한 내용은 크기를 초과한 구성 항목 변경 알림 예를 참조하세요.

AWS Config 는에서 사용하는 Amazon S3 버킷에 대한 AWS KMS 암호화를 지원합니다. AWS Config

AWS Key Management Service (AWS KMS) 키 또는 별칭 Amazon 리소스 이름(ARN)을 제공하여 Amazon Simple Storage Service(Amazon S3) 버킷으로 전송되는 데이터를 암호화할 수 있습니다. 기본적으로는 구성 기록 및 스냅샷 파일을 Amazon S3 버킷으로 AWS Config 전송하고 S3 AES-256 서버 측 암호화인 SSE-S3를 사용하여 저장 데이터를 암호화합니다. 그러나 AWS Config 에 KMS 키 또는 별칭 ARN을 제공하는 경우는 AES-256 암호화 대신 해당 KMS 키를 AWS Config 사용합니다.

AWS Config 는 기본 보존이 활성화된 상태에서 객체 잠금이 활성화된 Amazon S3 버킷으로의 전송 채널을 지원하지 않습니다. 자세한 내용은 S3 객체 잠금 작동 방식을 참조하세요.

용어

구성 항목은 계정에 있는 지원되는 AWS 리소스의 다양한 속성에 대한 point-in-time 보기를 나타냅니다. 구성 항목의 구성 요소에는 메타데이터, 속성, 관계, 현재 구성 및 관련 이벤트가 포함됩니다.는 기록 중인 리소스 유형에 대한 변경을 감지할 때마다 구성 항목을 AWS Config 생성합니다. 예를 들어 AWS Config 가 Amazon S3 버킷을 기록하는 경우는 버킷이 생성, 업데이트 또는 삭제될 때마다 구성 항목을 AWS Config 생성합니다. 에 대해 AWS Config 를 선택하여 설정한 기록 빈도로 구성 항목을 생성할 수도 있습니다.

구성 기록은 임의의 기간 동안 지정된 리소스에 대한 구성 항목의 모음입니다. 구성 기록을 통해 리소스가 처음 생성된 시간, 리소스가 지난 한 달간 구성된 방법, 어제 오전 9시에 도입된 구성 변경에 대한 질문에 답할 수 있습니다. 구성 기록은 여러 형식으로 제공됩니다.는 사용자가 지정한 Amazon S3 버킷에 기록되는 각 리소스 유형에 대한 구성 기록 파일을 AWS Config 자동으로 전송합니다. AWS Config 콘솔에서 지정된 리소스를 선택하고 타임라인을 사용하여 해당 리소스의 모든 이전 구성 항목으로 이동할 수 있습니다. 또한 API에서 리소스의 구성 기록 항목에 액세스할 수도 있습니다.

구성 스냅샷은 계정에 있는 지원되는 리소스에 대한 구성 항목의 모음입니다. 이 구성 스냅샷은 기록 중인 리소스와 그 구성의 전체 사진입니다. 구성 스냅샷은 구성의 유효성을 검사할 때 유용한 도구일 수 있습니다. 예를 들어, 잘못 구성되었거나 없어야 하는 리소스의 구성 스냅샷을 정기적으로 검토하고자 할 수 있습니다. 구성 스냅샷은 여러 형식으로 제공됩니다. 구성 스냅샷이 지정한 Amazon Simple Storage Service(S3) 버킷으로 전달되도록 할 수 있습니다. 또한 AWS Config 콘솔에서 특정 시점을 선택하고 리소스 간의 관계를 사용하여 구성 항목의 스냅샷을 탐색할 수 있습니다.

구성 스트림은 기록 중인 리소스에 대한 모든 구성 항목의 자동 업데이트 목록 AWS Config 입니다. 리소스가 생성, 수정 또는 삭제될 때마다 AWS Config 는 구성 항목을 만들고 구성 스트림에 추가합니다. 구성 스트림은 선택한 Amazon Simple Notification Service(SNS) 주제를 사용하여 작동합니다. 구성 스트림은 잠재적인 문제를 발견하거나, 특정 리소스가 변경되면 알림을 생성하거나, 리소스 구성을 반영해야 하는 외부 시스템을 업데이트할 수 있도록 구성 변경 사항이 발생할 때 이를 관찰하는 데 유용합니다 AWS .

구성 항목의 구성 요소

구성 항목은 계정에 있는 지원되는 AWS 리소스의 다양한 속성에 대한 point-in-time 보기를 나타냅니다. 구성 항목의 구성 요소에는 메타데이터, 속성, 관계, 현재 구성 및 관련 이벤트가 포함됩니다.는 기록 중인 리소스 유형에 대한 변경을 감지할 때마다 구성 항목을 AWS Config 생성합니다. 예를 들어 AWS Config 가 Amazon S3 버킷을 기록하는 경우는 버킷이 생성, 업데이트 또는 삭제될 때마다 구성 항목을 AWS Config 생성합니다. 에 대해 AWS Config 를 선택하여 설정한 기록 빈도로 구성 항목을 생성할 수도 있습니다.

구성 항목은 다음 구성 요소로 구성됩니다.

구성 요소	설명	포함
메타데이터	이 구성 항목에 대한 정보	• 버전 ID • 구성 항목이 캡처된 시간 • 항목이 캡처되었는지 여부를 나타내는 구성 항목의 상태 • 리소스의 구성 항목 순서를 나타내는 상태 ID
속성	Resource attributes	• 리소스 ID • 이 리소스의 키-값 태그 목록 • 리소스 유형(에 대해 지원되는 리소스 유형 AWS Config 참조) • Amazon 리소스 이름(ARN) • 이 리소스가 포함된 가용 영역(해당되는 경우) • 리소스가 생성된 시간
관계	해당 리소스와 계정에 연결된 다른 리소스와의 관계	관계에 대한 설명(예: Amazon EBS 볼륨 `vol-1234567` 은 Amazon EC2 인스턴스 `i-a1b2c3d4` 에 연결됨)
현재 구성	리소스의 Describe API 또는 List API로의 호출을 통해 반환되는 정보	예를 들어, `DescribeVolumes` API는 해당 볼륨에 대한 다음 정보를 반환합니다. • 볼륨이 위치한 가용 영역

구성 요소	설명	포함
		• 볼륨이 연결된 시간 • EC2 인스턴스가 연결된 ID • 볼륨의 현재 상태 • DeleteOnTermination 플래그의 상태 • 볼륨이 연결된 디바이스 • 볼륨의 유형(예: `gp2`, `io1`, 또는 `standard`)

Notes

1. 구성 항목 관계에는 네트워크 흐름 또는 데이터 흐름 종속성은 포함되지 않습니다. 구성 항목은 애플리케이션 아키텍처를 나타내도록 사용자 지정할 수 없습니다.
2. 버전 1.3부터, relatedEvents 필드는 비어 있습니다. AWS CloudTrail API 참조의 LookupEvents API에 액세스하여 리소스에 대한 이벤트를 검색할 수 있습니다.
3. 버전 1.3부터, configurationItemMD5Hash 필드는 비어 있습니다. configurationStateId 필드를 사용하여 구성 항목이 최신 상태인지 확인할 수 있습니다.
4. 리소스 유형이 태그 지정을 지원하지 않거나 API 응답 설명에 태그 정보를 포함하지 않는 경우 AWS Config 는 해당 리소스 유형의 구성 항목(CIs)에 태그 데이터를 캡처하지 않습니다. AWS Config 는 여전히 이러한 리소스를 기록합니다. 그러나 태그 데이터에 의존하는 기능은 작동하지 않습니다. 이는 태그 데이터에 의존하는 태그 기반 필터링, 그룹화 또는 규정 준수 평가에 영향을 미칩니다.

전송 채널 보기

전송 채널 AWS CLI 에 대한 세부 정보를 보려면를 사용해야 합니다.

다음 코드 예시는 `DescribeDeliveryChannels`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

전송 채널에 대한 세부 정보를 가져오려면

다음 명령은 전송 채널에 대한 세부 정보를 반환합니다.

```
aws configservice describe-delivery-channels
```

출력:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeDeliveryChannels 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제는 리전의 전송 채널을 검색하고 세부 정보를 표시합니다.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

출력:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- API 세부 정보는 Cmdlet 참조(V4)의 DescribeDeliveryChannels를 참조하세요. AWS Tools for PowerShell

전송 채널 업데이트

전송 채널을 업데이트할 때 다음 옵션을 설정할 수 있습니다.

- 가 구성 스냅샷과 구성 기록 파일을 AWS Config 전송하는 Amazon S3 버킷입니다.
- 가 Amazon S3 버킷에 구성 스냅샷을 AWS Config 전송하는 빈도입니다.
- 가 구성 변경에 대한 알림을 AWS Config 보내는 Amazon SNS 주제입니다.

전송 채널을 업데이트(콘솔)

AWS Config 콘솔을 사용하여 전송 채널에 대한 Amazon S3 버킷과 Amazon SNS 주제를 설정할 수 있습니다. 이러한 설정을 관리하는 단계는 콘솔 AWS Config 로 설정 섹션을 참조하세요.

이 콘솔은 전송 채널 이름을 바꾸거나, 구성 스냅샷의 빈도를 설정하거나, 전송 채널을 삭제하기 위한 옵션을 제공하지 않습니다. 이러한 작업을 수행하려면 AWS CLI, AWS Config API 또는 SDKs 중 AWS 하나를 사용해야 합니다.

전송 채널(AWS SDKs)을 업데이트하려면

다음 코드 예시는 `PutDeliveryChannel`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

전송 채널을 생성하려면

다음 명령은 전송 채널에 대한 설정을 JSON 코드로 제공합니다.

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

`deliveryChannel.json` 파일이 전송 채널 속성을 지정합니다.

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

이 예에서는 다음 속성을 설정합니다.

name - 전송 채널의 이름입니다. 기본적으로 AWS 구성은 `default` 새 전송 채널에 이름을 할당합니다. `put-delivery-channel` 명령을 사용하여 전송 채널 이름을 업데이트할 수 없습니다. 이름을 변경하는 단계는 전송 채널 이름 변경을 참조하세요.`s3BucketName` - AWS Config가 구성 스냅샷 및 구성 기록 파일을 전송하는 Amazon S3 버킷의 이름입니다. 다른 AWS 계정에 속하는 버킷을 지정하는 경우 해당 버킷에는 AWS Config에 액세스 권한을 부여하는 정책이 있어야 합니다. 자세한 내용을 알아보려면 Amazon S3 버킷에 대한 권한을 참조하세요.

`snsTopicARN` - AWS Config가 구성 변경에 대한 알림을 보내는 Amazon SNS 주제의 Amazon 리소스 이름(ARN)입니다. 다른 계정에서 주제를 선택하는 경우 주제에 AWS Config에 액세스 권한을 부여하는 정책이 있어야 합니다. 자세한 내용은 SNS 주제에 대한 권한을 참조하세요.

`configSnapshotDeliveryProperties` - Config가 구성 스냅샷을 전송하는 빈도와 주기적 AWS Config 규칙에 대한 평가를 호출하는 빈도를 설정하는 `deliveryFrequency` 속성을 포함합니다.

명령이 성공하면 AWS Config는 출력을 반환하지 않습니다. 전송 채널의 설정을 확인하려면 describe-delivery-channels 명령을 실행합니다.

- API 세부 정보는 AWS CLI 명령 참조의 PutDeliveryChannel 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제는 기존 전송 채널의 deliveryFrequency 속성을 변경합니다.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- API 세부 정보는 Cmdlet 참조(V4)의 PutDeliveryChannel을 참조하세요. AWS Tools for PowerShell

(선택 사항) 다음 `describe-delivery-channels` 명령을 사용하여 전송 채널 설정이 업데이트되었는지 확인할 수 있습니다.

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
```

```
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

다음 코드 예시는 `DescribeDeliveryChannels`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

전송 채널에 대한 세부 정보를 가져오려면

다음 명령은 전송 채널에 대한 세부 정보를 반환합니다.

```
aws configservice describe-delivery-channels
```

출력:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeDeliveryChannels 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제는 리전의 전송 채널을 검색하고 세부 정보를 표시합니다.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

출력:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- API 세부 정보는 Cmdlet 참조(V4)의 DescribeDeliveryChannels를 참조하세요. AWS Tools for PowerShell

전송 채널의 이름 바꾸기

전송 채널 이름을 변경하려면 이를 삭제한 후 원하는 이름의 새 전송 채널을 만들어야 합니다. 전송 채널을 삭제하기 전에 구성 레코더를 일시적으로 중지해야 합니다. AWS Config 콘솔은 전송 채널을 삭제하는 옵션을 제공하지 않습니다. AWS CLI, AWS Config API 또는 AWS SDKs 중 하나를 사용해야 합니다.

를 사용하여 전송 채널 이름 바꾸기 AWS CLI

1. 다음 `stop-configuration-recorder` 명령을 사용하여 구성 레코더를 중지합니다.

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

2. 다음 `describe-delivery-channels` 명령을 사용하고, 전송 채널의 속성을 적어둡니다.

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
```

```
    ]
}
```

3. 다음 delete-delivery-channel 명령을 사용하여 전송 채널을 삭제합니다.

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. 다음 put-delivery-channel 명령을 사용하여 원하는 이름의 전송 채널을 만듭니다.

```
$ aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

deliveryChannel.json 파일이 전송 채널 속성을 지정합니다.

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. 다음 `start-configuration-recorder` 명령을 사용하여 기록을 재개합니다.

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

구성 스냅샷을 Amazon S3 버킷에 전송

구성 스냅샷은 계정에 있는 지원되는 리소스에 대한 구성 항목의 모음입니다. 이 구성 스냅샷은 기록 중인 리소스와 그 구성의 전체 사진입니다. 구성 스냅샷은 구성의 유효성을 검사할 때 유용한 도구일 수 있습니다. 예를 들어, 잘못 구성되었거나 없어야 하는 리소스의 구성 스냅샷을 정기적으로 검토하고자 할 수 있습니다. 구성 스냅샷은 여러 형식으로 제공됩니다. 구성 스냅샷이 지정한 Amazon Simple Storage Service(S3) 버킷으로 전달되도록 할 수 있습니다. 또한 AWS Config 콘솔에서 특정 시점을 선택하고 리소스 간의 관계를 사용하여 구성 항목의 스냅샷을 탐색할 수 있습니다.

구성 스냅샷 전송

AWS Config 는 DeliverConfigSnapshot 작업을 호출하거나 명령을 실행할 때 구성 스냅샷을 AWS CLI `deliver-config-snapshot` 생성합니다.는 활성화할 때 지정한 Amazon S3 버킷에 구성 스냅샷을 AWS Config 저장합니다 AWS Config.

전송 채널을 구성할 AWS Config 때에서 할당한 이름을 지정하여 `deliver-config-snapshot` 명령을 입력합니다. 예:

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

전송 상태 확인

`describe-delivery-channel-status` 명령을 입력하여 AWS Config 가 지정된 전송 채널로 구성을 전송하기 시작했는지 확인합니다.

```
aws configservice describe-delivery-channel-status
```

응답에는가 버킷 및 주제에 구성을 전달하는 데 AWS Config 사용하는 세 가지 전송 형식의 상태가 모두 나열됩니다.

```
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
```

```
            },
            "name": "default"
        }
    ]
}
```

configSnapshotDeliveryInfo에서 lastSuccessfulTime 필드를 봅니다. 그 시간이 구성 스냅샷의 전송을 마지막으로 요청한 시간과 일치해야 합니다.

> **Note**
>
> AWS Config 는 UTC 형식(협정 세계시)을 사용하여 시간을 기록합니다.

Amazon S3 버킷의 구성 스냅샷 확인

구성 스냅샷은 계정에 있는 지원되는 리소스에 대한 구성 항목의 모음입니다. 이 구성 스냅샷은 기록 중인 리소스와 그 구성의 전체 사진입니다. 구성 스냅샷은 구성의 유효성을 검사할 때 유용한 도구일 수 있습니다. 예를 들어, 잘못 구성되었거나 없어야 하는 리소스의 구성 스냅샷을 정기적으로 검토하고자 할 수 있습니다. 구성 스냅샷은 여러 형식으로 제공됩니다. 구성 스냅샷이 지정한 Amazon Simple Storage Service(S3) 버킷으로 전달되도록 할 수 있습니다. 또한 AWS Config 콘솔에서 특정 시점을 선택하고 리소스 간의 관계를 사용하여 구성 항목의 스냅샷을 탐색할 수 있습니다.

구성 스냅샷 확인

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/s3/ Amazon S3 콘솔을 엽니다.
2. Amazon S3 콘솔의 모든 버킷 목록에서 Amazon S3 버킷 이름을 클릭합니다.
3. 명령으로 반환된 ID와 동일한 스냅샷 ID를 가진 ConfigSnapshot 객체가 나타날 때까지 버킷의 중첩 폴더를 클릭해 내려갑니다. 객체를 다운로드하고 열어 구성 스냅샷을 봅니다. 또한 S3 버킷에는 라는 빈 파일이 포함되어 있습니다ConfigWritabilityCheckFile.는 서비스가 S3 버킷에 성공적으로 쓸 수 있는지 확인하기 위해이 파일을 AWS Config 생성합니다.

의 구성 스냅샷 예제 AWS Config

다음은 구성 스냅샷에가 AWS Config 포함된 정보의 예입니다. 스냅샷은의 현재 리전에서 기록 AWS Config 중인 리소스에 대한 구성을 설명하고 이러한 리소스 간의 관계를 AWS 계정설명합니다.

> **Note**
>
> 구성 스냅샷에는 지원되지 않는 리소스 유형과 리소스 ID에 대한 참조가 포함될 수 있습니다.


```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
```

```
                    "instanceId": "i-344c463d",
                    "device": "/dev/sdf",
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "i-344c463d",
        "accountId": "12345678910",
        "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
        "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
        "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-adb69edbb1e4",
            "c376e30d-71a2-4694-89b7-a5a04ad92281"
        ],
        "availibilityZone": "us-west-2b",
        "resourceType": "AWS::EC2::Instance",
        "resourceCreationTime": "2014-02-26T22:56:35.000Z",
        "tags": {
            "Name": "integ-test-1",
            "examplename": "examplevalue"
        },
        "relationships": [
            {
                "resourceId": "vol-ce676ccc",
                "resourceType": "AWS::EC2::Volume",
                "name": "Attached Volume"
```

```
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
                "monitoring": {
                    "state": "disabled"
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
```

```
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
                ],
                "virtualizationType": "paravirtual",
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
```

```
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
```

```
            }
        }
    ]
}
```

다음 단계는 구성 스냅샷이 전송 채널로 전송되었는지 확인하는 것입니다.

가 Amazon SNS 주제로 AWS Config 보내는 알림

> **Note**
>
> AWS Config 가 Amazon SNS 주제에 알림을 보내려면 먼저 구성 레코더와 전송 채널을 설정해야 합니다. 자세한 내용은 구성 레코더 관리 및 전송 채널 관리를 참조하세요.

구성 변경 및 알림을 Amazon SNS 주제로 스트리밍 AWS Config 하도록를 구성할 수 있습니다. 예를 들어, 리소스가 업데이트되면 변경 사항을 볼 수 있도록 이메일로 전송되는 알림을 받을 수 있습니다. 가 사용자 지정 또는 관리형 규칙을 리소스와 비교하여 AWS Config 평가할 때 알림을 받을 수도 있습니다. 자세한 내용은 에서 로깅 및 모니터링을 AWS Config 참조하세요.

AWS Config 는 다음 이벤트에 대한 알림을 보냅니다.

- 리소스의 구성 항목 변경
- 리소스에 대한 구성 기록이 계정에 전달되었을 때
- 기록된 리소스에 대한 구성 스냅샷이 시작되어 계정에 전달되었을 때
- 리소스의 준수 상태와 규칙 준수 여부
- 리소스와 대조하여 규칙에 대한 평가를 시작했을 때
- AWS Config 가 계정에 알림을 전송하지 못했습니다.

주제

- 구성 항목 변경 알림의 예시
- 구성 기록 전달 알림 예
- 구성 스냅샷 전달 시작 알림 예
- 구성 스냅샷 전달 알림 예
- 준수 변경 알림 예
- 규칙 평가 시작 알림 예

- 크기를 초과한 구성 항목 변경 알림 예
- 전달 실패 알림 예

구성 항목 변경 알림의 예시

AWS Config 는 Amazon SNS를 사용하여 구독 엔드포인트에 알림을 전송합니다. 이러한 알림은 구성 스냅샷 및 구성 기록에 대한 전송 상태를 제공하고, 기록된 AWS 리소스의 구성이 변경될 때 AWS Config 가 생성하는 각 구성 항목을 제공합니다. AWS Config 또한는 리소스가 규칙을 준수하는지 여부를 보여주는 알림을 보냅니다. 이메일로 알림을 전송하도록 선택하면 사용자의 이메일 클라이언트 애플리케이션에서 이메일의 제목 줄 및 메시지 본문에 기초해 필터를 사용할 수 있습니다.

다음은 Amazon Elastic Block Store 볼륨 `vol-ce676ccc`와 ID가 `i-344c463d`인 인스턴스가 연결되었음을 AWS Config 가 감지했을 때 생성되는 Amazon SNS 알림의 페이로드 예시입니다. 알림에는 해당 리소스의 구성 항목 변경이 포함됩니다.

```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "awsAccountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
```

```
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [],
                "volumeType": "standard"
            }
        }
    ],
    "configurationItemDiff": {
        "changeType": "UPDATE",
        "changedProperties": {
            "Configuration.State": {
                "previousValue": "available",
                "updatedValue": "in-use",
                "changeType": "UPDATE"
            },
            "Configuration.Attachments.0": {
                "updatedValue": {
                    "VolumeId": "vol-ce676ccc",
                    "InstanceId": "i-344c463d",
                    "Device": "/dev/sdf",
                    "State": "attached",
                    "AttachTime": "FriMar0723: 46: 28UTC2014",
                    "DeleteOnTermination": "false"
                },
                "changeType": "CREATE"
            }
```

```
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```

관계를 보유한 리소스의 구성 항목

리소스가 다른 리소스에 관련되어 있으면 전자를 변경했을 때 구성 항목이 여러 개 발생할 수 있습니다. 다음 예제에서는가 관계가 있는 리소스에 대한 구성 항목을 AWS Config 생성하는 방법을 보여줍니다.

1. ID가 `i-007d374c8912e3e90`인 Amazon EC2 인스턴스가 있으며 이 인스턴스는 Amazon EC2 보안 그룹 와 연결되어 있습니다.
2. 사용자는 EC2 인스턴스를 업데이트해 보안 그룹을 다른 보안 그룹인 `sg-3f1fef43`으로 변경합니다.
3. EC2 인스턴스는 다른 리소스와 관련이 있으므로는 다음 예제와 같은 여러 구성 항목을 AWS Config 생성합니다.

이 알림에는 보안 그룹이 교체될 때 EC2 인스턴스에 적용된 구성 항목 변경 사항이 포함되어 있습니다.

```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
```

```
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "updatedValue": null,
```

```
                    "changeType": "DELETE"
                },
                "Relationships.0": {
                    "previousValue": {
                        "resourceId": "sg-c8b141b4",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Configuration.NetworkInterfaces.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-2",
                            "groupId": "sg-3f1fef43"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
```

```
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.0": {
                    "previousValue": {
                        "groupName": "example-security-group-1",
                        "groupId": "sg-c8b141b4"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                }
            },
            "changeType": "UPDATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [
```

```
                {
                    "resourceId": "eni-fde9493f",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::NetworkInterface",
                    "name": "Contains NetworkInterface"
                },
                {
                    "resourceId": "sg-3f1fef43",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::SecurityGroup",
                    "name": "Is associated with SecurityGroup"
                },
                {
                    "resourceId": "subnet-2372be7b",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Subnet",
                    "name": "Is contained in Subnet"
                },
                {
                    "resourceId": "vol-0a2d63a256bce35c5",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Is attached to Volume"
                },
                {
                    "resourceId": "vpc-14400670",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::VPC",
                    "name": "Is contained in Vpc"
                }
            ],
            "configuration": {
                "instanceId": "i-007d374c8912e3e90",
                "imageId": "ami-9be6f38c",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-16-84.ec2.internal",
                "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "ec2-micro",
                "amiLaunchIndex": 0,
                "productCodes": [],
```

```
                "instanceType": "t2.micro",
                "launchTime": "2017-01-09T20:13:28.000Z",
                "placement": {
                    "availabilityZone": "us-east-2c",
                    "groupName": "",
                    "tenancy": "default",
                    "hostId": null,
                    "affinity": null
                },
                "kernelId": null,
                "ramdiskId": null,
                "platform": null,
                "monitoring": {"state": "disabled"},
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "privateIpAddress": "172.31.16.84",
                "publicIpAddress": "54.175.43.43",
                "stateReason": null,
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/xvda",
                "blockDeviceMappings": [{
                    "deviceName": "/dev/xvda",
                    "ebs": {
                        "volumeId": "vol-0a2d63a256bce35c5",
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:03.000Z",
                        "deleteOnTermination": true
                    }
                }],
                "virtualizationType": "hvm",
                "instanceLifecycle": null,
                "spotInstanceRequestId": null,
                "clientToken": "bIYqA1483990561516",
                "tags": [{
                    "key": "Name",
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
```

```
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "sourceDestCheck": true,
                    "groups": [{
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
```

```
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


이 알림에는 EC2 인스턴스와 연결된 EC2 보안 그룹 `sg-3f1fef43`의 구성 항목 변경 사항이 포함되어 있습니다.


```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
```

```
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
```

```
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Amazon SNS **`ConfigurationItemChangeNotification`** 알림의 **`configurationItemDiff`** 필드 이해

AWS Config 는 리소스의 구성이 변경될 때마다 구성 항목을 생성합니다(create/update/delete). 에서 기록할 AWS Config 수 있는 지원되는 리소스 유형 목록은 섹션을 참조하세요에 대해 지원되는 리소스 유형 AWS Config. AWS Config 는 Amazon SNS를 사용하여 변경 사항이 발생할 때 알림을 전송합니다. Amazon SNS 알림 페이로드에는 지정된 AWS 리전의 리소스 변경 사항을 추적하는 데 도움이 되는 필드가 포함되어 있습니다.

`ConfigurationItemChangeNotification` 알림을 받는 이유를 이해하려면 `configurationItemDiff` 세부 정보를 검토하세요. 필드는 변경 유형에 따라 다르며 UPDATE-UPDATE, UPDATE-CREATE, DELETE-DELETE 등 다양한 조합을 구성할 수 있습니다. 다음은 몇 가지 일반적인 조합에 대한 설명입니다.

UPDATE-CREATE 및 UPDATE-UPDATE

다음 예제는 리소스 직접 관계 및 리소스 구성의 변경 사항을 포함합니다. `configurationItemDiff` 세부 정보에는 다음 정보가 표시됩니다.

수행된 작업: 계정에 있는 관리형 정책이 AWS Identity and Access Management (IAM) 역할에 연결되었습니다.

수행된 기본 작업: UPDATE(계정 내 `AWS::IAM::Policy` 리소스 유형의 연결 수 업데이트)입니다.

변경 유형 조합:

1. 리소스 직접 관계 변경 UPDATE-CREATE입니다. IAM 정책과 IAM 역할 간에 새로운 연결 또는 연관이 생성되었습니다.
2. 리소스 구성 변경 UPDATE-UPDATE입니다. 정책이 IAM 역할에 연결될 때 IAM 정책 연결 수가 2에서 3으로 증가했습니다.

UPDATE-CREATE 및 UPDATE-UPDATE `configurationItemDiff` 알림 예제

```
{
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                >>>>>>>>>>>>>>>>>>>> 1
            },
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
                "changeType": "UPDATE"                >>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

UPDATE-DELETE

다음 예제는 리소스 직접 관계 및 리소스 구성의 변경 사항을 포함합니다. `configurationItemDiff` 세부 정보에는 다음 정보가 표시됩니다.

수행된 작업: 계정에 있는 관리형 정책이 IAM 사용자와 분리되었습니다.

수행된 기본 작업: UPDATE(`AWS::IAM::User` 리소스 유형에 연결된 권한 정책 업데이트)입니다.

변경 유형 조합: 리소스 직접 관계 변경 UPDATE-DELETE입니다. 계정의 IAM 사용자와 IAM 정책 간의 연결이 삭제되었습니다.

UPDATE-DELETE `configurationItemDiff` 알림 예제

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Configuration.UserPolicyList.0": {
        "previousValue": {
          "policyName": "Test2",
          "policyDocument": "{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/VPCId": "*"
                }
            }
        }
    ]
}"
        },
        "updatedValue": null,
        "changeType": "DELETE"                        >>>>>>>>>>>>>>>>>>>>> 3
      }
    },
    "changeType": "UPDATE"
  }
}
```

DELETE-DELETE

다음 예제는 리소스 직접 관계 및 리소스 구성의 변경 사항을 포함합니다. `configurationItemDiff` 세부 정보에는 다음 정보가 표시됩니다.

수행된 작업: 계정에 있는 IAM 역할이 삭제되었습니다.

수행된 기본 작업: DELETE(`AWS::IAM::Role` 리소스 유형의 리소스가 삭제됨)입니다.

변경 유형 조합: 리소스 직접 관계 변경 및 리소스 구성 변경 DELETE-DELETE입니다. IAM 역할을 삭제하여 IAM 정책과 IAM 역할 간 연결도 삭제되었습니다.

DELETE-DELETE `configurationItemDiff` 알림 예제

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Relationships.0": {
        "previousValue": {
          "resourceId": "ANPAIJ5MXUKK*********",
          "resourceName": "AWSCloudTrailAccessPolicy",
          "resourceType": "AWS::IAM::Policy",
          "name": "Is attached to CustomerManagedPolicy"
        },
        "updatedValue": null,
        "changeType": "DELETE"
      },
      "Configuration": {
        "previousValue": {
          "path": "/",
          "roleName": "CloudTrailRole",
          "roleId": "AROAJITJ6YGM*********",
          "arn": "arn:aws:iam::123456789012:role/CloudTrailRole",
          "createDate": "2017-12-06T10:27:51.000Z",
          "assumeRolePolicyDocument": "{"Version":"2012-10-17","Statement":
[{"Sid":"","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"sts:AssumeRole","Condition":
{"StringEquals":{"sts:ExternalId":"123456"}}}]}",
          "instanceProfileList": [],
          "rolePolicyList": [],
          "attachedManagedPolicies": [
            {
              "policyName": "AWSCloudTrailAccessPolicy",
              "policyArn": "arn:aws:iam::123456789012:policy/AWSCloudTrailAccessPolicy"
            }
          ],
          "permissionsBoundary": null,
          "tags": [],
          "roleLastUsed": null
        },
        "updatedValue": null,
```

```
        "changeType": "DELETE"
      }
    },
    "changeType": "DELETE"
}
```

구성 기록 전달 알림 예

구성 기록은 임의의 기간 동안 특정 리소스 유형에 대한 구성 항목의 모음입니다. 다음은 CloudTrail 추적 리소스의 구성 기록이 계정에 전달될 때가 AWS Config 전송하는 알림의 예입니다.

```
{
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

구성 스냅샷 전달 시작 알림 예

다음은가 계정의 구성 스냅샷을 전송하기 AWS Config 시작할 때가 AWS Config 보내는 알림의 예입니다.

```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


구성 스냅샷 전달 알림 예

구성 스냅샷은 계정의 모든 기록된 리소스와 그 구성에 대한 구성 항목의 모음입니다. 다음은 계정에 구성 스냅샷이 전달될 때가 AWS Config 보내는 알림의 예입니다.


```
{
    "Type": "Notification",
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
```

```
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb
+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/
TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


준수 변경 알림 예

가 사용자 지정 또는 관리형 규칙을 기준으로 리소스를 AWS Config 평가할 때 리소스가 규칙을 준수하는지 여부를 보여주는 알림을 AWS Config 보냅니다.

다음은 CloudTrail 추적 리소스가 `cloudtrail-enabled` 관리형 규칙을 준수한 경우의 알림 예입니다.


```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
```

```
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
```

```
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

예: Config 구성 항목 변경 | Amazon EventBridge

```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
```

```
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
```

```
    }
  }
}
```

규칙 평가 시작 알림 예

AWS Config 는 리소스에 대해 사용자 지정 또는 관리형 규칙을 평가하기 시작하면 알림을 보냅니다. 다음은가 `iam-password-policy` 관리형 규칙을 평가하기 AWS Config 시작할 때의 알림 예제입니다.

```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

크기를 초과한 구성 항목 변경 알림 예

가 리소스에 대한 구성 변경을 AWS Config 감지하면 구성 항목(CI) 알림을 보냅니다. 알림이 Amazon Simple Notification Service(SNS)에서 허용한 최대 크기를 초과하는 경우, 이 알림에는 해당 구성 항목에 대한 간략한 요약이 들어 있습니다.

`s3BucketLocation` 필드에 지정한 Amazon S3 버킷 위치에서 완료 알림을 볼 수 있습니다.

다음 예제 알림은 Amazon EC2 인스턴스의 CI를 보여줍니다. 이 알림에는 변경 요약과 Amazon S3 버킷에서의 알림 위치가 들어 있습니다.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z

    The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
```

```
        "s3BucketLocation": "amzn-s3-demo-bucket/AWSLogs/123456789012/
Config/us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

크기 초과 구성 항목에 액세스하는 방법

구성 항목이 크면 요약만 Amazon SNS로 전송됩니다. 전체 구성 항목(CI)은 Amazon S3에 저장됩니다.

다음 코드 예제에서는 전체 CI에 액세스하는 방법을 보여줍니다.

```
import boto3
import json

def handle_oversized_configuration_item(event):
    """
    Example of handling an oversized configuration item notification

    When a configuration item is oversized:
    1. AWS Config sends a summary notification through SNS
    2. The complete configuration item is stored in S3
    3. Use get_resource_config_history API to retrieve the complete configuration
    """

    # Extract information from the summary notification
    if event['messageType'] == 'OversizedConfigurationItemChangeNotification':
        summary = event['configurationItemSummary']
        resource_type = summary['resourceType']
        resource_id = summary['resourceId']

        # Initialize AWS Config client
        config_client = boto3.client('config')

        # Retrieve the complete configuration item
```

```
        response = config_client.get_resource_config_history(
            resourceType=resource_type,
            resourceId=resource_id
        )

        if response['configurationItems']:
            config_item = response['configurationItems'][0]

            # For EC2 instances, the configuration contains instance details
            configuration = json.loads(config_item['configuration'])
            print(f"Instance Configuration: {configuration}")

            # Handle supplementary configuration if present
            if 'supplementaryConfiguration' in config_item:
                for key, value in config_item['supplementaryConfiguration'].items():
                    if isinstance(value, str):
                        config_item['supplementaryConfiguration'][key] =
json.loads(value)
                print(f"Supplementary Configuration:
{config_item['supplementaryConfiguration']}")

            return config_item

        # If needed, you can also access the complete notification from S3
        s3_location = event['s3DeliverySummary']['s3BucketLocation']
        print(f"Complete notification available in S3: {s3_location}")

    return None
```

작동 방법

1. 함수는 AWS Config 알림이 포함된 이벤트 파라미터를 수락합니다.
2. 메시지 유형이 크기 초과 구성 알림인지 확인합니다.
3. 함수는 요약에서 리소스 유형과 ID를 추출합니다.
4. AWS Config 클라이언트를 사용하여 전체 구성 기록을 검색합니다.
5. 함수는 기본 구성과 보조 구성을 모두 처리합니다.
6. 필요한 경우 제공된 S3 위치에서 전체 알림에 액세스할 수 있습니다.

전달 실패 알림 예

AWS Config 가 Amazon S3 버킷에 구성 스냅샷 또는 크기 초과 구성 항목 변경 알림을 전송할 AWS Config 수 없는 경우는 전송 실패 알림을 보냅니다. 유효한 Amazon S3 버킷을 지정했는지 확인합니다.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    -----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
      "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
```

```
    "recordVersion": "1.0"
  }
```

AWS Config 대시보드 보기

대시보드를 사용하여 리소스, 규칙, 적합성 팩 및 규정 준수 상태에 대한 개요를 확인하고 Amazon CloudWatch를 사용하여 AWS Config 사용량 및 성공 지표를 시각화할 수 있습니다. 이 페이지에서는 계정 AWS 의 상위 리소스,의 규정 준수 수준이 가장 낮은 적합성 팩 AWS 계정,의 규정 미준수 규칙 또는 리소스 AWS 계정, AWS Config 사용량을 주도하는 트래픽, 워크플로에서 발생한 성공 및 실패에 대한 주요 지표를 빠르게 식별할 수 있습니다.

AWS Config 대시보드를 사용하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 대시보드를 선택합니다.

목차

- 규정 준수 및 리소스 인벤토리
- AWS Config 사용량 및 성공 지표

규정 준수 및 리소스 인벤토리

설정 후는 지정된 리소스를 기록하고 규칙에 따라 평가하기 AWS Config 시작합니다. AWS Config 가 리소스, 규칙, 적합성 팩 및 규정 준수 상태를 표시하는 데 몇 분 정도 걸릴 수 있습니다.

규정 준수 점수별 적합성 팩

규정 준수 점수별 적합성 팩에는 규정 준수 점수가 가장 낮은 적합성 팩이 최대 10개까지 표시됩니다. 규정 준수 점수는 적합성 팩의 가능한 총 규칙-리소스 조합 수와 비교한 적합성 팩의 규정 준수 규칙-리소스 조합 수의 백분율입니다.

이 지표는 적합성 팩의 규정 준수 상태를 개괄적으로 보여 주며, 적합성 팩의 규정 준수 수준을 식별, 조사 및 이해하는 데 사용할 수 있습니다. 규정 준수 점수를 사용하여 문제 해결 진행 상황을 추적하고, 다양한 요구 사항 세트를 비교하고, 특정 변경 또는 배포가 적합성 팩에 미치는 영향을 확인할 수 있습니다.

적합성 팩의 배포 상태, 규정 준수 점수, 규정 준수 점수 타임라인 및 규칙을 자세히 보려면 적합성 팩 아래에서 적합성 팩의 이름을 선택합니다.

규정 준수 상태

규정 준수 상태에는 규정 준수/미준수 규칙 및 규정 준수/미준수 리소스의 수가 표시됩니다. 리소스는 관련 규칙의 평가에 따라 규정 준수 또는 규정 미준수입니다. 리소스가 규칙 사양을 따르지 않는 경우 해당 리소스 및 규칙은 규정 미준수로 플래그가 지정됩니다.

규정 미준수 규칙 및 리소스의 목록을 보려면 규정 미준수 규칙 또는 규정 미준수 리소스를 선택합니다.

규정 미준수 리소스별 규칙

규정 미준수 리소스별 규칙은 상위 규정 미준수 규칙을 리소스 수를 기준으로 내림차순으로 표시합니다. 규칙을 선택하면 해당 규칙의 세부 정보, 파라미터 및 해당 규칙의 범위 내 리소스를 볼 수 있습니다.

규정 미준수 규칙의 전체 목록을 보려면 전체 규정 미준수 규칙 보기를 선택하세요.

리소스 인벤토리

리소스 인벤토리는 AWS Config 가 기록하는 총 리소스 수를 리소스 수와의 각 리소스 유형 수를 기준으로 내림차순으로 표시합니다 AWS 계정. 특정 리소스 유형의 리소스를 모두 열려면 해당 리소스 유형을 선택하여 리소스 인벤토리 페이지로 이동합니다.

드롭다운 목록을 사용하여 보려는 리소스 총계를 표시할 수 있습니다. 기본적으로 모든 리소스를 보도록 설정되지만 리소스, 타사 AWS 리소스 또는 사용자 지정 리소스로 변경할 수 있습니다.

> **Note**
>
> 다음과 같은 이유로 Config 규칙을 사용하여 AWS 리소스 구성 평가 메시지가 대시보드에 표시될 수 있습니다.
>
> - 에 대한 AWS Config 규칙을 설정하지 않았습니다 AWS 계정. 규칙 추가를 선택하여 규칙 페이지로 이동합니다.
> - AWS Config 는 여전히 규칙을 기준으로 리소스를 평가하고 있습니다. 페이지를 새로 고쳐서 최신 평가 결과를 볼 수 있습니다.
> - AWS Config 는 규칙을 기준으로 리소스를 평가했으며 범위에서 리소스를 찾지 못했습니다. 설정 페이지에서가 AWS Config 기록할 리소스를 지정할 수 있습니다. 자세한 내용은 [를 사용하여 AWS 리소스 기록 AWS Config](#) 단원을 참조하십시오.

AWS Config 사용량 및 성공 지표

AWS Config 콘솔에서 Amazon CloudWatch 대시보드를 사용하여 AWS Config 사용량 및 성공 지표를 시각화할 수 있습니다.

각 대시보드에서 다음을 수행할 수 있습니다.

- 대시보드 시간 범위를 조정하여 지난 3시간, 1일 또는 1주간의 데이터를 표시할 수 있습니다.
- 달력 아이콘을 선택하여 지정된 과거 시간 동안의 상대 시간 또는 두 날짜 사이의 절대 시간 범위와 같은 사용자 지정 시간 범위를 입력합니다.
- 시간 형식을 변경하여 대시보드 데이터를 UTC(협정 세계시) 또는 현지 시간대(현재 사용하는 컴퓨터의 운영 체제에서 현지 시간대로 지정된 시간대)로 표시할 수도 있습니다.
- 새로 고침 아이콘 옆의 드롭 화살표를 사용하여 대시보드의 데이터를 새로 고칠 빈도를 지정하거나 자동 새로 고침을 끕니다. 끄기, 10초, 1분, 2분, 5분 또는 15분을 선택하여 새로 고침 간격을 변경합니다.
- 추가 옵션(세로 줄임표 메뉴)을 선택하여 사용 AWS Config 지표 또는 AWS Config 대시보드에서 현재 보고 있는 AWS Config 성공 지표를 CloudWatch 콘솔에 추가합니다. 그러면 CloudWatch 콘솔에 현재 AWS Config 사용 지표 또는 AWS Config 성공 지표에서 복사된 정보를 사용하여 CloudWatch에서 새 사용자 지정 대시보드를 생성할 수 있는 새 탭이 열립니다.

CloudWatch를 사용하여 이러한 지표에 대한 추가 분석을 수행하려면 CloudWatch 콘솔의 왼쪽 탐색 창에서 지표를 선택한 다음 AWS/Config를 선택합니다. CloudWatch 콘솔에서 수행할 수 있는 작업에 대한 자세한 내용은 CloudWatch 사용 설명서의 Amazon CloudWatch 대시보드 사용 및 Amazon CloudWatch 지표 사용을 참조하세요.

AWS Config 사용량 지표

지표	설명	단위	
`Configuration Items Recorded`	각 리소스 유형 또는 모든 리소스 유형에 대해 기록된 구성 항목 수가 표시됩니다. 구성 항목은 지원되는 AWS 리소스의 다양한 속성에 대한 point-in-time 보기를 나타냅니다. 구성 항목 또는 지원되는 리소스 유형에 대한 자세한 내용은 구성 항목 및 지원되는 리소스 유형을 참조하세요.	개수	

드롭다운 목록을 사용하여 보려는 리소스 유형을 선택할 수 있습니다. 기본적으로 모든 리소스 유형을 보도록 설정되어 있습니다.

AWS Config 성공 지표

지표	설명	단위
`Change Notifications Delivery Failed`	전송 채널의 Amazon SNS 주제로 변경 알림 전송이 실패한 횟수가 표시됩니다. 변경 알림은 AWS 리소스의 구성 상태 변경에 대해 알려줍니다. ConfigStreamDeliveryInfo API를 사용하여 변경 알림에 대해 마지막으로 시도한 전송에 대한 `lastErrorCode` 또는 `lastErrorMessage` 값을 가져올 수 있습니다. 자세한 내용은 전송 채널 관리를 참조하세요.	개수
`Config History Export Failed`	실패한 구성 이력의 수를 Amazon S3 버킷으로 내보냅니다. 구성 이력은 지정된 기간 동안 지정된 리소스에 대한 구성 항목의 모음입니다. 구성 이력에 대한 자세한 내용은 구성 기록을 참조하세요.	개수
`Configuration Recorder Insufficient Permissions Failure`	계정의 모든 구성 레코더에 대한 IAM 역할 정책으로 인해 실패한 권한 액세스 시도 횟수 AWS 리전 이며 권한이 충분하지 않습니다. 구성 레코더는 범위의 리소스 유형에 대한의 변경 사항을 감지합니다. 구성 레코더가 AWS 리소스 구성을 기록하려면 필요한 IAM 권한이 필요합니다. 자세한 내용은 구성 세부 정보를 가져오기 위한 IAM 역할 정책을 참조하세요.	개수
`Config Snapshot Export Failed`	실패한 구성 스냅샷의 수를 Amazon S3 버킷으로 내보냅니다. 구성 스냅샷은 계정의 지원되는 리소스에 대한 구성 항목의 모음입니다. 구성 스냅샷에 대한 자세한 내용은 구성 스냅샷을 참조하세요.	개수

를 사용하여 AWS 리소스 구성 관리 및 보기 AWS Config

AWS Config 를 사용하면 AWS 리소스 구성을 평가, 감사 및 평가할 수 있습니다.

AWS 리소스는 AWS Management Console, AWS Command Line Interface (CLI), AWS SDKs. AWS 리소스의 AWS 예로는 Amazon EC2 인스턴스, 보안 그룹, Amazon VPCs 및 Amazon Elastic Block Store가 있습니다.는 리소스 ID 또는 Amazon 리소스 이름(ARN)과 같은 고유 식별자를 사용하여 각 리소스를 AWS Config 참조합니다.

일반적인 사용 사례는 다음과 같습니다.

- 클라우드 관리자: 리소스 구성을 추적 및 관리하여 규정 준수를 보장하고, 문제를 해결하며, AWS 환경에 대한 이해를 유지할 수 있습니다.
- 보안 분석가: 원하는 상태에 대해 리소스 구성을 평가하여 취약성을 식별하고 보안 태세를 평가할 수 있습니다.
- 규정 준수 책임자: 리소스 구성을 지속적으로 감사하고 모니터링하여 조직 정책 및 업계 표준을 준수할 수 있습니다.

주제

- 에 대해 지원되는 리소스 유형 AWS Config
- 리전 가용성별 리소스 범위
- 를 사용하여 AWS 리소스 기록 AWS Config
- 를 사용하여 타사 리소스 AWS Config 용를 사용하여 구성 기록 AWS CLI
- 를 사용하여 관리형 인스턴스에 대한 소프트웨어 구성 기록 AWS Config
- 에서 검색한 리소스 조회 AWS Config
- 를 사용하여 AWS 리소스에 대한 규정 준수 정보 및 평가 결과 보기 AWS Config
- 를 사용하여 AWS 리소스에 대한 규정 준수 기록 보기 AWS Config
- AWS 리소스에 대한 규정 준수 기록 쿼리
- AWS Config 리소스 태그 지정

에 대해 지원되는 리소스 유형 AWS Config

> **Important**
>
> 이 페이지는 매월 초에 월별 주기로 업데이트됩니다.

AWS Config 는 다음과 같은 AWS 리소스 유형 및 리소스 관계를 지원합니다.

- 리소스 유형에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS 리소스 및 속성 유형 참조에서 해당 참조 정보(예: 구문, 속성 및 반환 값)를 참조하세요.
- AWS Config 기록을 위해 일부 AWS 리전은 이러한 리소스 유형의 하위 집합을 지원합니다. 각 리전에서 지원되는 리소스 유형에 대한 자세한 내용은 리전 가용성별 리소스 적용 범위를 참조하세요.
- 에 대한 고급 쿼리는 이러한 리소스 유형의 하위 집합을 AWS Config 지원합니다. 이러한 지원되는 리소스 유형 목록은 지원되는 리소스 유형을 참조하세요.
- 에 대한 사전 평가는 이러한 리소스 유형의 하위 집합을 AWS Config 지원합니다. 지원되는 리소스 유형 목록은 사전 평가에 지원되는 리소스 유형을 참조하세요.
- 주기적 규칙은 구성 항목(CIs)에 의존하지 않으므로 구성 레코더를 활성화하지 않고 주기적 규칙이 실행됩니다. 변경 트리거 규칙과 주기적 규칙의 차이점에 대한 자세한 내용은 평가 모드 및 AWS Config 규칙의 트리거 유형을 참조하세요.

  즉, 규칙 페이지를 보면 나열된 CI 또는 지원되는 리소스가 없습니다. 리소스 ID를 선택하면 오류가 표시됩니다`The provided resource ID and resource type cannot be found`. 이는 예상된 동작입니다.

> **Note**
>
> 리소스 유형에 대한 리전 가용성
> 추적할 리소스 유형을 지정 AWS Config 하기 전에 리전 가용성별 리소스 적용 범위를 확인하여 설정한 AWS 리전에서 리소스 유형이 지원되는지 확인합니다 AWS Config. 리소스 유형이 하나 이상의 리전 AWS Config 에서에서 지원되는 경우, 설정한 리전에서 AWS Config지정된 리소스 유형이 지원되지 않더라도에서 지원하는 모든 AWS 리전에서 해당 리소스 유형의 기록을 활성화할 수 있습니다 AWS Config.
> 리소스 유형에 대한 태그 지정 지원
> 리소스 유형이 태그 지정을 지원하지 않거나 API 응답 설명에 태그 정보를 포함하지 않는 경우 AWS Config 는 해당 리소스 유형의 구성 항목(CIs)에 태그 데이터를 캡처하지 않습니다. AWS

Config 는 여전히 이러한 리소스를 기록합니다. 그러나 태그 데이터에 의존하는 기능은 작동하지 않습니다. 이는 태그 데이터에 의존하는 태그 기반 필터링, 그룹화 또는 규정 준수 평가에 영향을 미칩니다.

Amazon 앱Stream

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon 앱Stream	`AWS::AppStream::DirectoryConfig`	NA	NA
	`AWS::AppStream::Application`	NA	NA
	`AWS::AppStream::Stack`	NA	NA
	`AWS::AppStream::Fleet`	NA	NA

Amazon AppFlow

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon AppFlow	`AWS::AppFlow::Flow`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon AppIntegrations	`AWS::AppIntegratio`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`ns::Event Integration`		
	`AWS::AppIntegrations::Application`	NA	NA

Amazon API Gateway

AWS 서비스	리소스 유형 값	관계	관련 리소스
API Gateway	`AWS::ApiGateway::Stage`	다음에 포함됨	ApiGateway Rest Api
		다음과 관련됨	WAFRegional WebACL
	`AWS::ApiGateway::RestApi`	다음을 포함함	ApiGateway Stage
API Gateway V2	`AWS::ApiGatewayV2::Stage`	다음에 포함됨	ApiGatewayV2 API
	`AWS::ApiGatewayV2::Api`	contains	ApiGatewayV2 Stage

가 Amazon API Gateway와 AWS Config 통합되는 방법에 대한 자세한 내용은 [를 사용하여 API Gateway API 구성 모니터링을 AWS Config](참조하세요.)

Amazon Athena

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Athena	`AWS::Athena::WorkGroup`	NA	NA
	`AWS::Athena::DataCatalog`	NA	NA
	`AWS::Athena::PreparedStatement`	NA	NA

Amazon Bedrock

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Bedrock	`AWS::Bedrock::Guardrail`	NA	NA
	`AWS::Bedrock::KnowledgeBase`	NA	NA

Amazon CloudFront

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon CloudFront	`AWS::CloudFront::Distribution`	다음과 관련됨	AWS WAF WebACL
			ACM 인증서
			S3 Bucket

AWS 서비스	리소스 유형 값	관계	관련 리소스
			IAM 서버 인증서
	`AWS::CloudFront::StreamingDistribution`	다음과 관련됨	AWS WAF WebACL
			ACM 인증서
			S3 Bucket
			IAM 서버 인증서

Amazon CloudWatch

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	NA	NA
	`AWS::CloudWatch::MetricStream`	NA	NA
Amazon CloudWatch Logs	`AWS::Logs::Destination`	NA	NA
Amazon CloudWatch RUM	`AWS::RUM::AppMonitor`	NA	NA
Amazon CloudWatch Evidently	`AWS::Evidently::Project`	NA	NA
	`AWS::Evidently::Launch`	NA	NA
	`AWS::Evidently::Segment`	NA	NA

Amazon CodeGuru

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon CodeGuru Reviewer	`AWS::CodeGuruReviewer::RepositoryAssociation`	NA	NA
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	NA	NA

Amazon Cognito

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Cognito	`AWS::Cognito::UserPool`	NA	NA
	`AWS::Cognito::UserPoolClient`	NA	NA
	`AWS::Cognito::UserPoolGroup`	NA	NA
	`AWS::Cognito::IdentityPool`	NA	NA

Amazon Connect

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Connect	`AWS::Connect::PhoneNumber`	NA	NA
	`AWS::Connect::QuickConnect`	NA	NA
	`AWS::Connect::Instance`	NA	NA
	`AWS::Connect::Rule`	NA	NA
	`AWS::Connect::User`	NA	NA
Amazon Connect Customer Profiles	`AWS::CustomerProfiles::Domain`	NA	NA
	`AWS::CustomerProfiles::ObjectType`	NA	NA

Amazon Detective

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Detective	`AWS::Detective::Graph`	NA	NA

Amazon DynamoDB

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon DynamoDB	`AWS::DynamoDB::Table`	NA	NA

Amazon Elastic Compute Cloud

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Elastic Compute Cloud	`AWS::EC2::Host` *	contains	EC2 인스턴스
	`AWS::EC2::EIP`	다음과 연결됨	EC2 인스턴스
			네트워크 인터페이스
	`AWS::EC2::Instance`	contains	EC2 네트워크 인터페이스
		다음과 관련됨	EC2 보안 그룹
		다음과 연결됨	Amazon EBS 볼륨
			EC2 엘라스틱 IP(EIP)
		다음에 포함됨	EC2 전용 호스트
			라우팅 테이블
			서브넷
			Virtual Private Cloud(VPC)
	`AWS::EC2::NetworkInterface`	다음과 관련됨	EC2 보안 그룹
		다음과 연결됨	EC2 엘라스틱 IP(EIP)

AWS 서비스	리소스 유형 값	관계	관련 리소스
			EC2 인스턴스
		다음에 포함됨	라우팅 테이블
			서브넷
			Virtual Private Cloud(VPC)
	`AWS::EC2::SecurityGroup` *	다음과 관련됨	EC2 인스턴스
			EC2 네트워크 인터페이스
			Virtual Private Cloud(VPC)
	`AWS::EC2::NatGateway`	다음에 포함됨	Virtual Private Cloud(VPC)
		다음에 포함됨	서브넷
	`AWS::EC2::EgressOnlyInternetGateway`	다음과 연결됨	Virtual Private Cloud(VPC)
	`AWS::EC2::EC2Fleet`	NA	NA
	`AWS::EC2::SpotFleet`	NA	NA
	`AWS::EC2::PrefixList`	NA	NA
	`AWS::EC2::FlowLog`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	AWS::EC2::TransitGateway	NA	NA
	AWS::EC2::TransitGatewayAttachment	NA	NA
	AWS::EC2::TransitGatewayRouteTable	NA	NA
	AWS::EC2::VPCEndpoint	다음에 포함됨	Virtual Private Cloud(VPC)
		다음과 연결됨	네트워크 인터페이스
		다음에 포함됨	서브넷
		다음에 포함됨	라우팅 테이블
	AWS::EC2::VPCEndpointService	다음과 관련됨	ElasticLoadBalancingV2 LoadBalancer
	AWS::EC2::VPCPeeringConnection	다음과 관련됨	Virtual Private Cloud(VPC)
	AWS::EC2::RegisteredHAInstance	다음과 관련됨	EC2 인스턴스

AWS 서비스	리소스 유형 값	관계	관련 리소스
	AWS::EC2::SubnetRouteTableAssociation	NA	NA
	AWS::EC2::LaunchTemplate	NA	NA
	AWS::EC2::NetworkInsightsAccessScopeAnalysis	NA	NA
	AWS::EC2::TrafficMirrorTarget	NA	NA
	AWS::EC2::TrafficMirrorSession	NA	NA
	AWS::EC2::DHCPOptions	NA	NA
	AWS::EC2::IPAM	NA	NA
	AWS::EC2::IPAMResourceDiscovery	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	AWS::EC2::IPAMResourceDiscoveryAssociation	NA	NA
	AWS::EC2::NetworkInsightsPath	NA	NA
	AWS::EC2::TrafficMirrorFilter	NA	NA
	AWS::EC2::CapacityReservation	NA	NA
	AWS::EC2::ClientVpnEndpoint	NA	NA
	AWS::EC2::CustomerGateway	다음과 연결됨	VPN 연결
	AWS::EC2::InternetGateway	다음과 연결됨	Virtual Private Cloud(VPC)
	AWS::EC2::NetworkAcl	NA	NA
	AWS::EC2::RouteTable	contains	EC2 인스턴스
			EC2 네트워크 인터페이스

AWS 서비스	리소스 유형 값	관계	관련 리소스
			서브넷
			VPN 게이트웨이
		다음에 포함됨	Virtual Private Cloud(VPC)
	`AWS::EC2::Subnet`	contains	EC2 인스턴스
			EC2 네트워크 인터페이스
		다음과 연결됨	네트워크 ACL
		다음에 포함됨	라우팅 테이블
			Virtual Private Cloud(VPC)
	`AWS::EC2::VPC`	contains	EC2 인스턴스
			EC2 네트워크 인터페이스
			네트워크 ACL
			라우팅 테이블
			서브넷
		다음과 관련됨	보안 그룹
		다음과 연결됨	인터넷 게이트웨이
			VPN 게이트웨이
	`AWS::EC2::VPNConnection`	다음과 연결됨	고객 게이트웨이
			VPN 게이트웨이

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::EC2::VPNConnectionRoute`	NA	NA
	`AWS::EC2::VPNGateway`	다음과 연결됨	Virtual Private Cloud(VPC)
			VPN 연결
		다음에 포함됨	라우팅 테이블
	`AWS::EC2::IPAMScope`	NA	NA
	`AWS::EC2::CarrierGateway`	NA	NA
	`AWS::EC2::TransitGatewayConnect`	NA	NA
	`AWS::EC2::IPAMPool`	NA	NA
	`AWS::EC2::TransitGatewayMulticastDomain`	NA	NA
	`AWS::EC2::NetworkInsightsAccessScope`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	AWS::EC2::NetworkInsightsAnalysis	NA	NA
	AWS::EC2::VPCBlockPublicAccessOptions	NA	NA
	AWS::EC2::VPCBlockPublicAccessExclusion	NA	NA
	AWS::EC2::EIPAssociation	NA	NA
	AWS::EC2::InstanceConnectEndpoint	NA	NA
	AWS::EC2::SnapshotBlockPublicAccess	NA	NA
	AWS::EC2::VPCEndpointConnectionNotification	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Elastic Block Store	`AWS::EC2::Volume`	다음과 연결됨	EC2 인스턴스
EC2 Image Builder	`AWS::ImageBuilder::ImagePipeline`	NA	NA
	`AWS::ImageBuilder::DistributionConfiguration`	NA	NA
	`AWS::ImageBuilder::ContainerRecipe`	NA	NA
	`AWS::ImageBuilder::InfrastructureConfiguration`	NA	NA
	`AWS::ImageBuilder::ImageRecipe`	NA	NA

*AWS Config 전용 호스트의 구성 세부 정보와 해당 호스트에서 시작하는 인스턴스를 기록합니다. 따라서 서버 바운드 소프트웨어 라이선스 준수를 보고할 때를 데이터 소스 AWS Config 로 사용할 수 있습니다. 예를 들어, 인스턴스의 구성 기록을 보고 그것이 기반으로 하는 Amazon 머신 이미지(AMI)를 확인할 수 있습니다. 그런 다음 소켓 및 코어 수 등의 세부 정보가 포함된 해당 호스트의 구성 기록을 찾아 호스트가 AMI의 라이선스 요구 사항을 준수하는지 확인할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 AWS Config를 사용하여 구성 변경 추적을 참조하세요.

*EC2 SecurityGroup 속성 정의에는 내부적으로 IP 범위로 변환되는 IP CIDR 블록이 포함되어 있으며, 특정 IP 범위를 찾으려고 할 때 예상치 못한 결과가 반환될 수 있습니다. 특정 IP 범위를 검색하기 위한 해결 방법은 고급 쿼리 제한 사항을 참조하세요.

Amazon Elastic 컨테이너 레지스트리

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Elastic 컨테이너 레지스트리	`AWS::ECR::Repository`	NA	NA
	`AWS::ECR::RegistryPolicy`	NA	NA
	`AWS::ECR::PullThroughCacheRule`	NA	NA
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	NA	NA

Amazon Elastic Container Service

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Elastic Container Service	`AWS::ECS::Cluster`	NA	NA
	`AWS::ECS::TaskDefinition`	NA	NA
	`AWS::ECS::Service` *	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::ECS::TaskSet`	NA	NA
	`AWS::ECS::Capacity Provider`	NA	NA

*이 서비스는 현재 새로운 Amazon 리소스 이름(ARN) 형식만 지원합니다. 자세한 내용은 ESC 개발자 안내서의 Amazon 리소스 이름(ARN) 및 ID 문서를 참조하세요.

이전 형식(지원되지 않음): `arn:aws:ecs:region:aws_account_id:service/service-name`

신규(지원됨): `arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`

Amazon Elastic File System

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Elastic File System	`AWS::EFS::FileSystem`	NA	NA
	`AWS::EFS::AccessPoint`	NA	NA

Amazon Elastic Kubernetes 서비스

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Elastic Kubernetes 서비스	`AWS::EKS::Cluster`	NA	NA
	`AWS::EKS::FargateProfile`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::EKS::IdentityProviderConfig`	NA	NA
	`AWS::EKS::Addon`	NA	NA

Amazon EMR

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon EMR	`AWS::EMR::SecurityConfiguration`	NA	NA

Amazon EventBridge

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon EventBridge	`AWS::Events::EventBus`	NA	NA
	`AWS::Events::ApiDestination`	NA	NA
	`AWS::Events::Archive`	NA	NA
	`AWS::Events::Endpoint`	NA	NA
	`AWS::Events::Connection`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::Events::Rule`	NA	NA
Amazon EventBridge 스키마	`AWS::EventSchemas::RegistryPolicy`	NA	NA
	`AWS::EventSchemas::Discoverer`	NA	NA
	`AWS::EventSchemas::Schema`	NA	NA
	`AWS::EventSchemas::Registry`	NA	NA

Amazon Forecast

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Forecast	`AWS::Forecast::Dataset`	NA	NA
	`AWS::Forecast::DatasetGroup`	NA	NA

Amazon Fraud Detector

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Fraud Detector	`AWS::FraudDetector::Label`	NA	NA
	`AWS::FraudDetector::EntityType`	NA	NA
	`AWS::FraudDetector::Variable`	NA	NA
	`AWS::FraudDetector::Outcome`	NA	NA

Amazon GuardDuty

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon GuardDuty	`AWS::GuardDuty::Detector`	NA	NA
	`AWS::GuardDuty::ThreatIntelSet`	NA	NA
	`AWS::GuardDuty::IPSet`	NA	NA
	`AWS::GuardDuty::Filter`	NA	NA

Amazon Inspector

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Inspector	`AWS::InspectorV2::Filter`	NA	NA
	`AWS::InspectorV2::Activation`	NA	NA

Amazon Interactive Video Service

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Interactive Video Service	`AWS::IVS::Channel`	NA	NA
	`AWS::IVS::RecordingConfiguration`	NA	NA
	`AWS::IVS::PlaybackKeyPair`	NA	NA

Amazon Keyspaces(Apache Cassandra용)

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Keyspaces (Apache Cassandra용)	`AWS::Cassandra::Keyspace`	NA	NA

Amazon OpenSearch Service

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon OpenSearch Service(레거시 Elasticsearch)	`AWS::Elasticsearch::Domain`	다음과 관련됨	KMS 키
			EC2 보안 그룹
			EC2 서브넷
			Virtual Private Cloud(VPC)
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`	NA	NA
Amazon OpenSearch Serverless	`AWS::OpenSearchServerless::VpcEndpoint`	NA	NA
	`AWS::OpenSearchServerless::Collection`	NA	NA

Amazon OpenSearch Service 이름 변경

2021년 9월 8일, Amazon Elasticsearch Service 이름이 Amazon OpenSearch Service로 변경되었습니다. OpenSearch Service는 OpenSearch 및 레거시 Elasticsearch OSS를 지원합니다. 자세한 내용은 Amazon OpenSearch Service - 변경 사항 요약을 참조하세요.
하나 이상의 도메인을 OpenSearch로 업그레이드하더라도 기존 `AWS::Elasticsearch::Domain` 리소스 유형`AWS::OpenSearch::Domain`에서 몇 주 동안에 대한 데이터를 계속 볼 수 있습니다.

Amazon Personalize

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Personalize	`AWS::Personalize::Dataset`	NA	NA
	`AWS::Personalize::Schema`	NA	NA
	`AWS::Personalize::Solution`	NA	NA
	`AWS::Personalize::DatasetGroup`	NA	NA

Amazon Pinpoint

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Pinpoint	`AWS::Pinpoint::ApplicationSettings`	NA	NA
	`AWS::Pinpoint::Segment`	NA	NA
	`AWS::Pinpoint::App`	NA	NA
	`AWS::Pinpoint::Campaign`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::Pinpoint::InAppTemplate`	NA	NA
	`AWS::Pinpoint::EmailChannel`	NA	NA
	`AWS::Pinpoint::EmailTemplate`	NA	NA
	`AWS::Pinpoint::EventStream`	NA	NA

Amazon Quantum Ledger Database(QLDB)

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon QLDB	`AWS::QLDB::Ledger`	NA	NA

Amazon Kendra

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Kendra	`AWS::Kendra::Index`	NA	NA

Amazon Kinesis

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Kinesis	`AWS::Kinesis::Stream`	NA	NA
	`AWS::Kinesis::StreamConsumer`	NA	NA
Amazon Kinesis Analytics V2	`AWS::KinesisAnalyticsV2::Application`	NA	NA
Amazon Data Firehose	`AWS::KinesisFirehose::DeliveryStream`	NA	NA
Kinesis 비디오 스트림	`AWS::KinesisVideo::SignalingChannel`	NA	NA
	`AWS::KinesisVideo::Stream`	NA	NA

Amazon Lex

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Lex	`AWS::Lex::BotAlias`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::Lex::Bot`	NA	NA

Amazon Lightsail

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Lightsail	`AWS::Lightsail::Disk`	NA	NA
	`AWS::Lightsail::Certificate`	NA	NA
	`AWS::Lightsail::Bucket`	NA	NA
	`AWS::Lightsail::StaticIp`	NA	NA

Amazon Lookout for Metrics

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Lookout for Metrics	`AWS::LookoutMetrics::Alert`	NA	NA

Amazon Lookout for Vision

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Lookout for Vision	`AWS::LookoutVision::Project`	NA	NA

Amazon Macie

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Macie	`AWS::Macie::Session`	NA	NA

Amazon Managed Grafana

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Managed Grafana	`AWS::Grafana::Workspace`	NA	NA

Amazon Managed Service for Prometheus

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Managed Service for Prometheus	`AWS::APS::RuleGroupsNamespace`	NA	NA

Amazon MemoryDB

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon MemoryDB	`AWS::MemoryDB::SubnetGroup`	NA	NA

Amazon MQ

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon MQ	`AWS::AmazonMQ::Broker`	NA	NA

Amazon Managed Streaming for Apache Kafka

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Managed Streaming for Apache Kafka	`AWS::MSK::Cluster`	NA	NA
	`AWS::MSK::Configuration`	NA	NA
	`AWS::MSK::BatchScramSecret`	NA	NA
	`AWS::MSK::ClusterPolicy`	NA	NA
	`AWS::MSK::VpcConnection`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Managed Streaming for Apache Kafka Connect	`AWS::KafkaConnect::Connector`	NA	NA

Amazon QuickSight

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon QuickSight	`AWS::QuickSight::DataSource`	NA	NA
	`AWS::QuickSight::Template`	NA	NA
	`AWS::QuickSight::Theme`	NA	NA

Amazon Redshift

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Redshift	`AWS::Redshift::Cluster`	다음과 관련됨	클러스터 파라미터 그룹
			클러스터 보안 그룹
			클러스터 서브넷 그룹
			보안 그룹
			Virtual Private Cloud(VPC)

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::Redshift::ClusterParameterGroup`	NA	NA
	`AWS::Redshift::ClusterSecurityGroup`	NA	NA
	`AWS::Redshift::ScheduledAction`	NA	NA
	`AWS::Redshift::ClusterSnapshot`	다음과 관련됨	클러스터
			Virtual Private Cloud(VPC)
	`AWS::Redshift::ClusterSubnetGroup`	다음과 관련됨	서브넷
			Virtual Private Cloud(VPC)
	`AWS::Redshift::EventSubscription`	NA	NA
	`AWS::Redshift::EndpointAccess`	NA	NA
	`AWS::Redshift::EndpointAuthorization`	NA	NA

Amazon Relational Database Service

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Relational Database Service	`AWS::RDS::DBInstance`	다음과 관련됨	EC2 보안 그룹
			RDS DB 보안 그룹
			RDS DB 서브넷 그룹
	`AWS::RDS::DBSecurityGroup`	다음과 관련됨	EC2 보안 그룹
			Virtual Private Cloud(VPC)
	`AWS::RDS::DBSnapshot`	다음과 관련됨	Virtual Private Cloud(VPC)
	`AWS::RDS::DBSubnetGroup`	다음과 관련됨	EC2 보안 그룹
			Virtual Private Cloud(VPC)
	`AWS::RDS::EventSubscription`	NA	NA
	`AWS::RDS::DBCluster`	contains	RDS DB 인스턴스
		다음과 관련됨	RDS DB 서브넷 그룹
			EC2 보안 그룹
	`AWS::RDS::DBClusterSnapshot`	다음과 관련됨	RDS DB 클러스터
			Virtual Private Cloud(VPC)
	`AWS::RDS::GlobalCluster`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	AWS::RDS::OptionGroup	NA	NA

Amazon Route 53

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Route 53	AWS::Route53::HostedZone	NA	NA
	AWS::Route53::HealthCheck	NA	NA
Amazon Route 53 프로필	AWS::Route53Profiles::Profile	NA	NA
Amazon Route 53 Resolver	AWS::Route53Resolver::ResolverEndpoint	NA	NA
	AWS::Route53Resolver::ResolverRule	NA	NA
	AWS::Route53Resolver::ResolverRuleAssociation	NA	NA
	AWS::Route53Resolver::FirewallDomainList	NA	NA
	AWS::Route53Resolver::FirewallRuleGroupAssociation	NA	NA
	AWS::Route53Resolver::ResolverQueryLoggingConfig	NA	NA
	AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	NA	NA
	AWS::Route53Resolver::FirewallRuleGroup	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Application Recovery Controller(ARC)	`AWS::Route53RecoveryReadiness::Cell`	NA	NA
	`AWS::Route53RecoveryReadiness::ReadinessCheck`	NA	NA
	`AWS::Route53RecoveryReadiness::RecoveryGroup`	NA	NA
	`AWS::Route53RecoveryControl::Cluster`	NA	NA
	`AWS::Route53RecoveryControl::ControlPanel`	NA	NA
	`AWS::Route53RecoveryControl::RoutingControl`	NA	NA
	`AWS::Route53RecoveryControl::SafetyRule`	NA	NA
	`AWS::Route53RecoveryReadiness::ResourceSet`	NA	NA

Amazon SageMaker AI

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon SageMaker AI	`AWS::SageMaker::CodeRepository`	NA	NA
	`AWS::SageMaker::Domain`	NA	NA
	`AWS::SageMaker::AppImageConfig`	NA	NA
	`AWS::SageMaker::Image`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::SageMaker::Model`	NA	NA
	`AWS::SageMaker::NotebookInstance`	NA	NA
	`AWS::SageMaker::NotebookInstanceLifecycleConfig`	NA	NA
	`AWS::SageMaker::EndpointConfig`	NA	NA
	`AWS::SageMaker::Workteam`	NA	NA
	`AWS::SageMaker::FeatureGroup`	NA	NA
	`AWS::SageMaker::InferenceExperiment`	NA	NA

Amazon Simple Email Service

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Simple Email Service	`AWS::SES::ConfigurationSet`	NA	NA
	`AWS::SES::ContactList`	NA	NA
	`AWS::SES::Template`	NA	NA
	`AWS::SES::ReceiptFilter`	NA	NA
	`AWS::SES::ReceiptRuleSet`	NA	NA

Amazon Simple Notification Service

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Simple Notification Service	`AWS::SNS::Topic`	NA	NA

Amazon Simple Queue Service

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Simple Queue Service	`AWS::SQS::Queue`	NA	NA

Amazon Simple Storage Service(S3)

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon Simple Storage Service(S3)	`AWS::S3::Bucket` *	NA	NA
	`AWS::S3::AccountPublicAccessBlock`	NA	NA
	`AWS::S3::MultiRegionAccessPoint`	NA	NA
	`AWS::S3::StorageLens`	NA	NA
	`AWS::S3::AccessPoint`	NA	NA
	`AWS::S3::StorageLensGroup`	NA	NA
Amazon S3 Express One Zone	`AWS::S3Express::DirectoryBucket`	NA	NA
	`AWS::S3Express::BucketPolicy`	NA	NA

*S3 버킷을 기록 AWS Config 하도록를 구성했는데 구성 변경 알림이 수신되지 않는 경우 S3 버킷 정책에 필요한 권한이 있는지 확인합니다. 자세한 내용은 S3 버킷 기록에 대한 권한 관리 단원을 참조하십시오.

Amazon S3 버킷 속성

AWS Config 는 Amazon S3 버킷 리소스 유형에 대해 다음 속성도 기록합니다.

속성	설명
AccelerateConfiguration	거리가 먼 클라이언트와 버킷 간의 데이터 Transfer Acceleration 입니다.
BucketAcl	버킷 및 객체에 대한 액세스를 관리하는 데 사용되는 ACL(액세스 제어 목록)입니다.
BucketPolicy	버킷에 대한 권한을 정의하는 정책입니다.
CrossOriginConfiguration	버킷에 cross-origin 요청을 허용합니다.
LifecycleConfiguration	버킷 내 객체의 수명 주기를 정의하는 규칙입니다.
LoggingConfiguration	버킷에 대한 액세스 요청을 추적하는 데 사용되는 로깅입니다.
NotificationConfiguration	지정된 버킷 이벤트에 대한 알림을 보내거나 워크플로를 트리거하는 데 사용되는 이벤트 알림입니다.
ReplicationConfiguration	여러 AWS 리전에 위치한 버킷 간에 객체를 자동 비동기식으로 복사하는 것입니다.
RequestPaymentConfiguration	요청자 지불이 사용하도록 설정되어 있습니다.
TaggingConfiguration	분류하기 위해 버킷에 추가된 태그입니다. 태깅을 사용하여 결제를 추적할 수도 있습니다.
WebsiteConfiguration	버킷에 정적 웹 사이트 호스팅이 활성화되어 있습니다.
VersioningConfiguration	버킷의 객체에 버전 관리가 활성화되어 있습니다.

속성에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 버킷 구성 옵션을 참조하세요.

Amazon WorkSpaces

AWS 서비스	리소스 유형 값	관계	관련 리소스
Amazon WorkSpaces	`AWS::WorkSpaces::ConnectionAlias`	NA	NA
	`AWS::WorkSpaces::Workspace`	NA	NA

AWS Amplify

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Amplify	`AWS::Amplify::App`	NA	NA
	`AWS::Amplify::Branch`	NA	NA

AWS AppConfig

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS AppConfig	`AWS::AppConfig::Application`	NA	NA
	`AWS::AppConfig::Environment`	NA	NA
	`AWS::AppConfig::Co`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	nfigurationProfile		
	AWS::AppConfig::DeploymentStrategy	NA	NA
	AWS::AppConfig::HostedConfigurationVersion	NA	NA
	AWS::AppConfig::ExtensionAssociation	NA	NA

AWS App Runner

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS App Runner	AWS::AppRunner::VpcConnector	NA	NA
	AWS::AppRunner::Service	NA	NA

AWS App Mesh

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS App Mesh	`AWS::AppMesh::VirtualNode`	NA	NA
	`AWS::AppMesh::VirtualService`	NA	NA
	`AWS::AppMesh::VirtualGateway`	NA	NA
	`AWS::AppMesh::VirtualRouter`	NA	NA
	`AWS::AppMesh::Route`	NA	NA
	`AWS::AppMesh::GatewayRoute`	NA	NA
	`AWS::AppMesh::Mesh`	NA	NA

AWS AppSync

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS AppSync	`AWS::AppSync::GraphQLApi`	NA	NA

AWS Audit Manager

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Audit Manager	`AWS::AuditManager::Assessment`	NA	NA

AWS Auto Scaling

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	contains	Amazon EC2 인스턴스
		다음과 관련됨	Classic Load Balancer
			Auto Scaling 시작 구성
			서브넷
	`AWS::AutoScaling::LaunchConfiguration`	다음과 관련됨	Amazon EC2 보안 그룹
	`AWS::AutoScaling::ScalingPolicy`	다음과 관련됨	Auto Scaling 그룹
			경보
	`AWS::AutoScaling::ScheduledAction`	다음과 관련됨	Auto Scaling 그룹

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::AutoScaling::WarmPool`	NA	NA

AWS Backup

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Backup	`AWS::Backup::BackupPlan`	NA	NA*
	`AWS::Backup::BackupSelection`	NA	NA
	`AWS::Backup::BackupVault`	NA	NA*
	`AWS::Backup::RecoveryPoint`	NA	NA
	`AWS::Backup::ReportPlan`	NA	NA

AWS Backup 작동 방식 때문에 이러한 리소스 유형 중 일부는이 표의 다른 AWS Backup 리소스 유형과 관련이 있습니다.

`AWS::Backup::BackupPlan`는 백업 계획에 선택 항목이 많은 `AWS::Backup::BackupSelection` 위치와 관련이 있으며, `AWS::Backup::BackupVault`는 AWS Backup 볼트에 복구 시점이 여러 개인 `AWS::Backup::RecoveryPoint` 위치와 관련이 있습니다.

자세한 내용은 백업 계획을 사용하여 백업 관리 및 AWS Backup로 작업하기 문서를 참조하세요.

AWS Batch

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Batch	`AWS::Batch::JobQueue`	NA	NA
	`AWS::Batch::ComputeEnvironment`	NA	NA
	`AWS::Batch::SchedulingPolicy`	NA	NA

AWS Budgets

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Budgets	`AWS::Budgets::BudgetsAction`	NA	NA

AWS Certificate Manager

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Certificate Manager	`AWS::ACM::Certificate`	NA	NA

AWS CloudFormation

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS CloudFormation	`AWS::CloudFormation::Stack` *	contains	지원되는 AWS 리소스 유형

*AWS Config 스택의 AWS CloudFormation 스택 및 지원되는 리소스 유형에 대한 구성 변경을 기록합니다. 아직 지원되지 AWS Config 않는 스택의 리소스 유형에 대한 구성 변경은 기록하지 않습니다. 지원되지 않는 리소스 유형은 스택에 대한 구성 항목의 보조 구성 섹션에 표시됩니다.

AWS CloudTrail

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS CloudTrail	`AWS::CloudTrail::Trail`	NA	NA

AWS Cloud9

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Cloud9	`AWS::Cloud9::EnvironmentEC2`	NA	NA

> **AWS Cloud9 신규 사용자가 더 이상 액세스할 수 없는 액세스**
>
> 신중한 고려 후 2024년 7월 25 AWS Cloud9일부터 새로운 고객 액세스를 종료하기로 결정했습니다. AWS Cloud9 기존 고객은 서비스를 정상적으로 계속 사용할 수 있습니다.는 보안, 가용성 및 성능 개선에 AWS 계속 투자 AWS Cloud9하지만 새로운 기능을 도입할 계획은 없습니다. 자세한 내용은 에서 AWS IDE 도구 키트 AWS Cloud9 로 마이그레이션하는 방법 또는 단원을 AWS CloudShell 참조하십시오.

AWS Cloud Map

AWS 서비스	리소스 유형 값	관계	관련 리소스
서비스 검색	`AWS::ServiceDiscovery::Service`	NA	NA
	`AWS::ServiceDiscovery::PublicDnsNamespace`	NA	NA
	`AWS::ServiceDiscovery::HttpNamespace`	NA	NA
`AWS::ServiceDiscovery::Instance`	NA	NA	

AWS CodeArtifact

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	NA	NA

AWS CodeBuild

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS CodeBuild	`AWS::CodeBuild::Project` *	다음과 관련됨	S3 버킷
			IAM 역할
	`AWS::CodeBuild::ReportGroup`	NA	NA

*가와 AWS Config 통합되는 방법에 대한 자세한 내용은 샘플 AWS Config 과 함께 AWS CodeBuild 사용을 AWS CodeBuild참조하세요.

AWS CodeDeploy

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS CodeDeploy	`AWS::CodeDeploy::Application`	contains	DeploymentGroup
	`AWS::CodeDeploy::DeploymentConfig`	NA	NA
	`AWS::CodeDeploy::DeploymentGroup`	다음에 포함됨	Application

AWS CodePipeline

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS CodePipeline	`AWS::CodePipeline::Pipeline` *	다음과 연결됨	S3 버킷
		다음과 관련됨	IAM 역할
			Code 프로젝트
			Lambda 함수
			Cloudformation 스택
			ElasticBeanstalk 애플리케이션

*AWS Config 파이프라인의 CodePipeline 파이프라인 및 지원되는 리소스 유형에 대한 구성 변경을 기록합니다. 아직 지원되지 AWS Config 않는 파이프라인의 리소스 유형에 대한 구성 변경은 기록하지 않습니다. `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, 및 `ECS service` 등과 같은 지원되지 않는 리소스 유형은 스택에 대한 구성 항목의 보조 구성 섹션에 표시됩니다.

AWS Config

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Config	`AWS::Config::ResourceCompliance` *	다음과 관련됨	모든 리소스*
	`AWS::Config::ConformancePackCompliance`	NA	NA
	`AWS::Config::Confi`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`gurationRecorder` *		

*`AWS::Config::ResourceCompliance`와 관련 리소스 간의 관계는 특정 리소스 유형에 대한 규정 준수를 `AWS::Config::ResourceCompliance`이 보고하는 방식에 따라 달라집니다.

*`AWS::Config::ConfigurationRecorder`는의 시스템 리소스 유형 AWS Config 이며이 리소스 유형의 기록은 기본적으로 활성화됩니다.

> **Note**
>
> `AWS::Config::ConformancePackCompliance` 및 `AWS::Config::ConfigurationRecorder` 리소스 유형 기록에는 추가 요금이 부과되지 않습니다.

AWS Database Migration Service

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Database Migration Service	`AWS::DMS::EventSubscription`	NA	NA
	`AWS::DMS::ReplicationSubnetGroup`	NA	NA
	`AWS::DMS::ReplicationInstance`	NA	NA
	`AWS::DMS::ReplicationTask`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::DMS::Certificate`	NA	NA
	`AWS::DMS::Endpoint`	NA	NA

AWS DataSync

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS DataSync	`AWS::DataSync::LocationSMB`	NA	NA
	`AWS::DataSync::LocationFSxLustre`	NA	NA
	`AWS::DataSync::LocationFSxWindows`	NA	NA
	`AWS::DataSync::LocationS3`	NA	NA
	`AWS::DataSync::LocationEFS`	NA	NA
	`AWS::DataSync::LocationNFS`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::DataSync::LocationHDFS`	NA	NA
	`AWS::DataSync::LocationObjectStorage`	NA	NA
	`AWS::DataSync::Task`	NA	NA

AWS Device Farm

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Device Farm	`AWS::DeviceFarm::TestGridProject`	NA	NA
	`AWS::DeviceFarm::InstanceProfile`	NA	NA
	`AWS::DeviceFarm::Project`	NA	NA

AWS Elastic Beanstalk

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Application`	contains	Elastic Beanstalk Application Version
			Elastic Beanstalk 환경
		다음과 관련됨	IAM 역할
	`AWS::ElasticBeanstalk::ApplicationVersion`	다음에 포함됨	Elastic Beanstalk 애플리케이션
		다음과 관련됨	Elastic Beanstalk 환경
			S3 버킷
	`AWS::ElasticBeanstalk::Environment`	다음에 포함됨	Elastic Beanstalk 애플리케이션
		다음과 관련됨	Elastic Beanstalk Application Version
			IAM 역할
		contains	CloudFormation 스택

AWS Fault Injection Service

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Fault Injection Service	`AWS::FIS::ExperimentTemplate`	NA	NA

AWS Global Accelerator

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	NA	NA
	`AWS::GlobalAccelerator::EndpointGroup`	NA	NA
	`AWS::GlobalAccelerator::Accelerator`	NA	NA

AWS Glue

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Glue	`AWS::Glue::Job`	NA	NA
	`AWS::Glue::Classifier`	NA	NA
	`AWS::Glue::MLTransform`	NA	NA

AWS Ground Station

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Ground Station	`AWS::GroundStation::Config`	NA	NA
	`AWS::GroundStation::MissionProfile`	NA	NA
	`AWS::GroundStation::DataflowEndpointGroup`	NA	NA

AWS HealthLake

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS HealthLake	`AWS::HealthLake::FHIRDatastore`	NA	NA

AWS Identity and Access Management (IAM)

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Identity and Access Management	`AWS::IAM::User`	다음과 연결됨	IAM 그룹
			IAM 고객 관리형 정책
	`AWS::IAM::Group`	contains	IAM 사용자

AWS 서비스	리소스 유형 값	관계	관련 리소스
		다음과 연결됨	IAM 고객 관리형 정책
	`AWS::IAM::Role`	다음과 연결됨	IAM 고객 관리형 정책
	`AWS::IAM::Policy`	다음과 연결됨	IAM 사용자
			IAM 그룹
			IAM 역할
	`AWS::IAM::SAMLProvider`	NA	NA
	`AWS::IAM::ServerCertificate`	NA	NA
	`AWS::IAM::InstanceProfile`	NA	NA
	`AWS::IAM::OIDCProvider`	NA	NA
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	NA	NA

AWS Config 에는 기록하는 구성 세부 정보와 함께 인라인 정책이 포함되어 있습니다. 인라인 정책에 대한 자세한 내용은 IAM 사용 설명서에서 관리형 정책과 인라인 정책 문서를 참조하세요.

AWS IoT

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS IoT	`AWS::IoT::Authorizer`	NA	NA
	`AWS::IoT::SecurityProfile`	NA	NA
	`AWS::IoT::RoleAlias`	NA	NA
	`AWS::IoT::Dimension`	NA	NA
	`AWS::IoT::Policy`	NA	NA
	`AWS::IoT::MitigationAction`	NA	NA
	`AWS::IoT::ScheduledAudit`	NA	NA
	`AWS::IoT::AccountAuditConfiguration`	NA	NA
	`AWS::IoTSiteWise::Gateway`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::IoT::CustomMetric`	NA	NA
	`AWS::IoT::JobTemplate`	NA	NA
	`AWS::IoT::ProvisioningTemplate`	NA	NA
	`AWS::IoT::CACertificate`	NA	NA
AWS IoT 무선	`AWS::IoTWireless::ServiceProfile`	NA	NA
	`AWS::IoTWireless::MulticastGroup`	NA	NA
	`AWS::IoTWireless::FuotaTask`	NA	NA
AWS IoT Core	`AWS::IoT::FleetMetric`	NA	NA
AWS IoT Analytics	`AWS::IoTAnalytics::Datastore`	NA	NA
	`AWS::IoTAnalytics::Dataset`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::IoTAnalytics::Pipeline`	NA	NA
	`AWS::IoTAnalytics::Channel`	NA	NA
AWS IoT Events	`AWS::IoTEvents::Input`	NA	NA
	`AWS::IoTEvents::DetectorModel`	NA	NA
	`AWS::IoTEvents::AlarmModel`	NA	NA
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`	NA	NA
	`AWS::IoTTwinMaker::Entity`	NA	NA
	`AWS::IoTTwinMaker::Scene`	NA	NA
	`AWS::IoTTwinMaker::SyncJob`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::IoTTwinMaker::ComponentType`	NA	NA
AWS IoT SiteWise	`AWS::IoTSiteWise::Dashboard`	NA	NA
	`AWS::IoTSiteWise::Project`	NA	NA
	`AWS::IoTSiteWise::Portal`	NA	NA
	`AWS::IoTSiteWise::AssetModel`	NA	NA
AWS IoT Greengrass Version 2	`AWS::GreengrassV2::ComponentVersion`	NA	NA

AWS Key Management Service

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Key Management Service	`AWS::KMS::Key`	NA	NA
	`AWS::KMS::Alias`	NA	NA

AWS Lambda

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Lambda	`AWS::Lambda::Function`	다음과 관련됨	IAM 역할
			EC2 보안 그룹
		다음에 포함됨	EC2 서브넷
	`AWS::Lambda::CodeSigningConfig`	NA	NA

AWS Mainframe Modernization

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Mainframe Modernization	`AWS::M2::Environment`	NA	NA

AWS Network Firewall

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	다음과 연결됨	EC2 서브넷
		다음과 관련됨	NetworkFirewall FirewallPolicy
	`AWS::NetworkFirewall::FirewallPolicy`	다음과 관련됨	NetworkFirewall RuleGroup

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::NetworkFirewall::RuleGroup`	NA	NA
	`AWS::NetworkFirewall::TLSInspectionConfiguration`	NA	NA
	`AWS::NetworkFirewall::VpcEndpointAssociation`	NA	NA

AWS Network Manager

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Network Manager	`AWS::NetworkManager::TransitGatewayRegistration`	NA	NA
	`AWS::NetworkManager::Site`	NA	NA
	`AWS::NetworkManager::Device`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::NetworkManager::Link`	NA	NA
	`AWS::NetworkManager::GlobalNetwork`	NA	NA
	`AWS::NetworkManager::CustomerGatewayAssociation`	NA	NA
	`AWS::NetworkManager::LinkAssociation`	NA	NA
	`AWS::NetworkManager::ConnectPeer`	NA	NA

AWS Panorama

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Panorama	`AWS::Panorama::Package`	NA	NA

AWS Private Certificate Authority

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`	NA	NA
	`AWS::ACMPCA::CertificateAuthorityActivation`	NA	NA

AWS Resilience Hub

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Resilience Hub	`AWS::ResilienceHub::ResiliencyPolicy`	NA	NA
	`AWS::ResilienceHub::App`	NA	NA

AWS 리소스 탐색기

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS 리소스 탐색기	`AWS::ResourceExplorer2::Index`	NA	NA

AWS RoboMaker

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS RoboMaker	`AWS::RoboMaker::RobotApplicationVersion`	NA	NA
	`AWS::RoboMaker::RobotApplication`	NA	NA
	`AWS::RoboMaker::SimulationApplication`	NA	NA

AWS Signer

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Signer	`AWS::Signer::SigningProfile`	NA	NA

AWS Secrets Manager

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Secrets Manager	`AWS::SecretsManager::Secret`	다음과 관련됨	Lambda 함수
		다음과 관련됨	KMS 키

AWS Security Hub

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Security Hub	`AWS::SecurityHub::Standard`	NA	NA

AWS Service Catalog

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Service Catalog	`AWS::ServiceCatalog::CloudFormationProduct`	다음에 포함됨	포트폴리오
		다음과 관련됨	CloudFormationProvisionedProduct
	`AWS::ServiceCatalog::CloudFormationProvisionedProduct`	다음과 관련됨	Portfolio
			CloudFormationProduct
			CloudFormationStack
	`AWS::ServiceCatalog::Portfolio`	contains	CloudFormationProduct

AWS Shield

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Shield	`AWS::Shield::Protection`	다음과 관련됨	Amazon CloudFront 배포

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::ShieldRegional::Protection`	다음과 관련됨	EC2 EIP
		다음과 관련됨	ElasticLoadBalancing Balancer
		다음과 관련됨	ElasticLoadBalancingV2 LoadBalancer

AWS Step Functions

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Step Functions	`AWS::StepFunctions::Activity`	NA	NA
	`AWS::StepFunctions::StateMachine`	NA	NA

AWS Systems Manager

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Systems Manager	`AWS::SSM::ManagedInstanceInventory` *	다음과 관련됨	EC2 인스턴스
	`AWS::SSM::PatchCompliance`	다음과 관련됨	관리형 인스턴스 인벤토리

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::SSM::AssociationCompliance`	다음과 관련됨	관리형 인스턴스 인벤토리
	`AWS::SSM::FileData`	다음과 관련됨	관리형 인스턴스 인벤토리
	`AWS::SSM::Document`	NA	NA

*관리형 인스턴스 인벤토리에 대해 자세히 알아보려면 Recording Software Configuration for Managed Instances 문서를 참조하세요.

AWS Transfer Family

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Transfer Family	`AWS::Transfer::Agreement`	NA	NA
	`AWS::Transfer::Connector`	NA	NA
	`AWS::Transfer::Workflow`	NA	NA
	`AWS::Transfer::Certificate`	NA	NA
	`AWS::Transfer::Profile`	NA	NA

AWS WAF

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS WAF	`AWS::WAF::RateBasedRule`	NA	NA
	`AWS::WAF::Rule`	NA	NA
	`AWS::WAF::WebACL`	다음과 관련됨	WAF 규칙
			WAF 비율 기반 규칙
			WAF Rulegroup
	`AWS::WAF::RuleGroup`	다음과 관련됨	WAF 규칙
	`AWS::WAFRegional::RateBasedRule`	NA	NA
	`AWS::WAFRegional::Rule`	NA	NA
	`AWS::WAFRegional::WebACL`	다음과 관련됨	ElasticLoadBalancingV2 LoadBalancer
			WAFRegional 규칙
			WAFRegional 비율 기반 규칙
			WAFRegional Rulegroup
	`AWS::WAFRegional::RuleGroup`	다음과 관련됨	WAFRegional 규칙

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS WAF V2	`AWS::WAFv2::WebACL`	다음과 관련됨	ElasticLoadBalancingV2 LoadBalancer
			ApiGateway Stage
			WAFv2 IPset
			WAFv2 RegexPatternSet
			WAFv2 RuleGroup
			WAFv2 ManagedRuleSet
	`AWS::WAFv2::RuleGroup`	다음과 관련됨	WAFv2 IPSet
			WAFv2 RegexPatternSet
	`AWS::WAFv2::ManagedRuleSet`	다음과 관련됨	WAFv2 RuleGroup
	`AWS::WAFv2::IPSet`	NA	NA
	`AWS::WAFv2::RegexPatternSet`	NA	NA

AWS X-Ray

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS X-Ray	`AWS::XRay::EncryptionConfig`	NA	NA

Elastic Load Balancing

AWS 서비스	리소스 유형 값	관계	관련 리소스
Elastic Load Balancing	Application Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	다음과 관련됨	EC2 보안 그룹
		다음과 연결됨	서브넷
		다음에 포함됨	Virtual Private Cloud(VPC)
	Application Load Balancer 리스너 `AWS::ElasticLoadBalancingV2::Listener`	NA	NA
	Classic Load Balancer `AWS::ElasticLoadBalancing::LoadBalancer`	다음과 관련됨	EC2 보안 그룹
		다음과 연결됨	서브넷
		다음에 포함됨	Virtual Private Cloud(VPC)
	Network Load Balancer	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`AWS::ElasticLoadBalancingV2::LoadBalancer`		

AWS Elemental MediaConnect

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Elemental MediaConnect	`AWS::MediaConnect::FlowEntitlement`	NA	NA
	`AWS::MediaConnect::FlowVpcInterface`	NA	NA
	`AWS::MediaConnect::FlowSource`	NA	NA
	`AWS::MediaConnect::Gateway`	NA	NA

AWS Elemental MediaPackage

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Elemental MediaPackage	`AWS::MediaPackage:`	NA	NA

AWS 서비스	리소스 유형 값	관계	관련 리소스
	`:PackagingGroup`		
	`AWS::MediaPackage::PackagingConfiguration`	NA	NA

AWS Elemental MediaTailor

AWS 서비스	리소스 유형 값	관계	관련 리소스
AWS Elemental MediaTailor	`AWS::MediaTailor::PlaybackConfiguration`	NA	NA

리전 가용성별 리소스 범위

북아메리카 및 남아메리카 리전

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::ACM::Certificate	예	예	예	예	예	예	예	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::ACMPCA::CertificateAuthority	예	예	예	예	예	예	아니요	예
AWS::ACMPCA::CertificateAuthorityActivation	예	예	예	예	예	예	아니요	예
AWS::APS::RuleGroupsNamespace	아니요	예	예	예	아니요	아니요	아니요	예
AWS::AccessAnalyzer::Analyzer	예	예	예	예	예	예	아니요	예
AWS::AmazonMQ::Broker	예	예	예	예	아니요	예	아니요	예
AWS::Amplify::App	예	예	예	예	아니요	예	아니요	예
AWS::Amplify::Branch	예	예	예	예	아니요	예	아니요	예
AWS::ApiGateway::RestApi	예	예	예	예	예	예	예	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::ApiGateway::Stage	예	예	예	예	예	예	예	예
AWS::ApiGatewayV2::Api	예	예	예	예	예	예	예	예
AWS::ApiGatewayV2::Stage	예	예	예	예	예	예	예	예
AWS::AppConfig::Application	예	예	예	예	아니요	예	아니요	예
AWS::AppConfig::ConfigurationProfile	예	예	예	예	아니요	예	아니요	예
AWS::AppConfig::DeploymentStrategy	예	예	예	예	예	예	아니요	예
AWS::AppConfig::Environment	예	예	예	예	아니요	예	아니요	예
AWS::AppConfig::ExtensionAssociation	예	예	예	예	예	예	아니요	예
AWS::AppConfig::HostedConfigurationVersion	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::AppFlow::Flow	예	예	예	예	아니요	예	아니요	예
AWS::AppIntegrations::Application	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::AppIntegrations::EventIntegration	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::AppMesh::GatewayRoute	예	예	예	예	아니요	예	아니요	예
AWS::AppMesh::Mesh	예	예	예	예	아니요	예	아니요	예
AWS::AppMesh::Route	예	예	예	예	아니요	예	아니요	예
AWS::AppMesh::VirtualGateway	예	예	예	예	아니요	예	아니요	예
AWS::AppMesh::VirtualNode	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::AppMesh::VirtualRouter	예	예	예	예	아니요	예	아니요	예
AWS::AppMesh::VirtualService	예	예	예	예	아니요	예	아니요	예
AWS::AppRunner::Service	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::AppRunner::VpcConnector	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::AppStream::Application	아니요	예	예	예	아니요	예	아니요	예
AWS::AppStream::DirectoryConfig	아니요	예	예	예	아니요	예	아니요	예
AWS::AppStream::Fleet	아니요	예	예	예	아니요	예	아니요	아니요
AWS::AppStream::Stack	아니요	예	예	예	아니요	예	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::AppSync::ApiCache	예	예	예	예	아니요	예	아니요	예
AWS::AppSync::GraphQLApi	예	예	예	예	아니요	예	아니요	예
AWS::Athena::DataCatalog	예	예	예	예	예	예	아니요	예
AWS::Athena::PreparedStatement	예	예	예	예	예	예	아니요	예
AWS::Athena::WorkGroup	예	예	예	예	예	예	아니요	예
AWS::AuditManager::Assessment	예	예	예	예	아니요	예	아니요	아니요
AWS::AutoScaling::AutoScalingGroup	예	예	예	예	예	예	예	예
AWS::AutoScaling::LaunchConfiguration	예	예	예	예	예	예	예	예
AWS::AutoScaling::ScalingPolicy	예	예	예	예	예	예	예	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::AutoScaling::ScheduledAction	예	예	예	예	예	예	예	예
AWS::Auto Scaling::WarmPool	예	예	예	예	아니요	예	아니요	예
AWS::Backup::BackupPlan	예	예	예	예	예	예	아니요	예
AWS::Back up::BackupSelection	예	예	예	예	예	예	아니요	예
AWS::Backup::BackupVault	예	예	예	예	예	예	아니요	예
AWS::Back up::RecoveryPoint	예	예	예	예	예	예	아니요	예
AWS::Backup::ReportPlan	예	예	예	예	아니요	예	아니요	예
AWS::Batch::Comput eEnvironment	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::Batch::JobQueue	예	예	예	예	아니요	예	아니요	예
AWS::Batch::SchedulingPolicy	예	예	예	예	예	예	아니요	예
AWS::Bedrock::Guardrail	아니요	예	예	예	아니요	예	아니요	예
AWS::Bedrock::KnowledgeBase	아니요	예	예	예	아니요	예	아니요	예
AWS::Budgets::BudgetsAction	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::Cassandra::Keyspace	예	예	예	예	아니요	예	아니요	예
AWS::Cloud9::EnvironmentEC2	예	예	예	예	아니요	예	아니요	예
AWS::CloudFormation::Stack	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::CloudFront::Distribution	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::CloudFront::StreamingDistribution	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::CloudTrail::Trail	예	예	예	예	예	예	예	예
AWS::CloudWatch::Alarm	예	예	예	예	예	예	예	예
AWS::CloudWatch::MetricStream	예	예	예	예	아니요	예	아니요	예
AWS::CodeArtifact::Repository	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::CodeBuild::Project	예	예	예	예	아니요	예	아니요	예
AWS::CodeBuild::ReportGroup	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::CodeDeploy::Application	예	예	예	예	아니요	예	아니요	예
AWS::CodeDeploy::DeploymentConfig	예	예	예	예	아니요	예	아니요	예
AWS::CodeDeploy::DeploymentGroup	예	예	예	예	아니요	예	아니요	예
AWS::CodeGuruProfiler::ProfilingGroup	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::CodeGuruReviewer::RepositoryAssociation	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::CodePipeline::Pipeline	예	예	예	예	아니요	예	아니요	예
AWS::Cognito::IdentityPool	예	예	예	예	예	예	아니요	예
AWS::Cognito::UserPool	예	예	예	예	예	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::Cognito::UserPoolClient	예	예	예	예	예	예	아니요	예
AWS::Cognito::UserPoolGroup	예	예	예	예	예	예	아니요	예
AWS::Config::ConfigurationRecorder	예	예	예	예	예	예	예	예
AWS::Config::ConformancePackCompliance	예	예	예	예	예	예	아니요	예
AWS::Config::ResourceCompliance	예	예	예	예	예	예	예	예
AWS::Connect::Instance	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::Connect::PhoneNumber	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::Connect::QuickConnect	아니요	예	예	아니요	아니요	예	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::Connect::Rule	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::Connect::User	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::CustomerProfiles::Domain	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::CustomerProfiles::ObjectType	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::DMS::Certificate	예	예	예	예	아니요	예	아니요	예
AWS::DMS::Endpoint	예	예	예	예	아니요	예	아니요	예
AWS::DMS::EventSubscription	예	예	예	예	아니요	예	아니요	예
AWS::DMS::ReplicationInstance	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::DMS::ReplicationSubnetGroup	예	예	예	예	아니요	예	아니요	예
AWS::DMS::ReplicationTask	예	예	예	예	아니요	예	아니요	예
AWS::DataSync::LocationEFS	예	예	예	예	아니요	예	아니요	예
AWS::DataSync::LocationFSxLustre	예	예	예	예	아니요	예	아니요	예
AWS::DataSync::LocationFSxWindows	예	예	예	예	아니요	예	아니요	예
AWS::DataSync::LocationHDFS	예	예	예	예	아니요	예	아니요	예
AWS::DataSync::LocationNFS	예	예	예	예	아니요	예	아니요	예
AWS::DataSync::LocationObjectStorage	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::DataSync::LocationS3	예	예	예	예	예	예	아니요	예
AWS::DataSync::LocationSMB	예	예	예	예	아니요	예	아니요	예
AWS::DataSync::Task	예	예	예	예	예	예	아니요	예
AWS::Detective::Graph	예	예	예	예	아니요	예	아니요	예
AWS::DeviceFarm::InstanceProfile	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::DeviceFarm::Project	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::DeviceFarm::TestGridProject	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::DynamoDB::Table	예	예	예	예	예	예	예	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::EC2::Capacity Reservation	예	예	예	예	예	예	아니요	예
AWS::EC2::CarrierGateway	아니요	예	예	예	아니요	예	아니요	아니요
AWS::EC2::ClientVpnEndpoint	예	예	예	예	아니요	예	아니요	예
AWS::EC2::ClientVpnTargetNetworkAssociation	예	예	예	예	아니요	예	아니요	예
AWS::EC2::CustomerGateway	예	예	예	예	예	예	예	예
AWS::EC2::DHCPOptions	예	예	예	예	예	예	아니요	예
AWS::EC2::EC2Fleet	예	예	예	예	아니요	예	아니요	예
AWS::EC2::EIP	예	예	예	예	예	예	예	예
AWS::EC2::EIPAssociation	예	예	예	예	예	예	예	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::EC2::EgressOnlyInternetGateway	예	예	예	예	아니요	예	아니요	예
AWS::EC2::FlowLog	예	예	예	예	아니요	예	아니요	예
AWS::EC2::Host	예	예	예	예	예	예	예	예
AWS::EC2::IPAM	예	예	예	예	아니요	예	아니요	예
AWS::EC2::IPAMPool	예	예	예	예	아니요	예	아니요	예
AWS::EC2::IPAMResourceDiscovery	예	예	예	예	아니요	예	아니요	예
AWS::EC2::IPAMResourceDiscoveryAssociation	예	예	예	예	아니요	예	아니요	예
AWS::EC2::IPAMScope	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::EC2::Instance	예	예	예	예	예	예	예	예
AWS::EC2::Instance ConnectEndpoint	예	예	예	예	예	예	아니요	예
AWS::EC2::InternetGateway	예	예	예	예	예	예	예	예
AWS::EC2::LaunchTemplate	예	예	예	예	아니요	예	아니요	예
AWS::EC2::NatGateway	예	예	예	예	아니요	예	아니요	예
AWS::EC2::NetworkAcl	예	예	예	예	예	예	예	예
AWS::EC2::NetworkInsightsAccessScope	예	예	예	예	아니요	예	아니요	예
AWS::EC2::NetworkInsightsAccessScopeAnalysis	예	예	예	예	아니요	예	아니요	예
AWS::EC2::NetworkInsightsAnalysis	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::EC2::NetworkInsightsPath	예	예	예	예	아니요	예	아니요	예
AWS::EC2::NetworkInterface	예	예	예	예	예	예	예	예
AWS::EC2::PrefixList	예	예	예	예	예	예	아니요	예
AWS::EC2::RegisteredHAInstance	예	예	예	예	아니요	예	아니요	예
AWS::EC2::RouteTable	예	예	예	예	예	예	예	예
AWS::EC2::SecurityGroup	예	예	예	예	예	예	예	예
AWS::EC2::SnapshotBlockPublicAccess	예	예	예	예	예	예	아니요	예
AWS::EC2::SpotFleet	예	예	예	예	예	예	아니요	예
AWS::EC2::Subnet	예	예	예	예	예	예	예	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::EC2::SubnetRouteTableAssociation	예	예	예	예	아니요	예	아니요	예
AWS::EC2::TrafficMirrorFilter	예	예	예	예	예	예	아니요	예
AWS::EC2::TrafficMirrorSession	예	예	예	예	아니요	예	아니요	예
AWS::EC2::TrafficMirrorTarget	예	예	예	예	아니요	예	아니요	예
AWS::EC2::TransitGateway	예	예	예	예	예	예	아니요	예
AWS::EC2::TransitGatewayAttachment	예	예	예	예	아니요	예	아니요	예
AWS::EC2::TransitGatewayConnect	예	예	예	예	아니요	예	아니요	예
AWS::EC2::TransitGatewayMulticastDomain	예	예	예	예	예	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::EC2::TransitGatewayRouteTable	예	예	예	예	아니요	예	아니요	예
AWS::EC2::VPC	예	예	예	예	예	예	예	예
AWS::EC2::VPCBlockPublicAccessExclusion	예	예	예	예	예	예	아니요	예
AWS::EC2::VPCBlockPublicAccessOptions	예	예	예	예	예	예	아니요	예
AWS::EC2::VPCEndpoint	예	예	예	예	예	예	예	예
AWS::EC2::VPCEndpointConnectionNotification	예	예	예	예	예	예	예	예
AWS::EC2::VPCEndpointService	예	예	예	예	예	예	예	예
AWS::EC2::VPCPeeringConnection	예	예	예	예	예	예	예	예
AWS::EC2::VPNConnection	예	예	예	예	예	예	예	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::EC2::VPNConnectionRoute	예	예	예	예	예	예	아니요	예
AWS::EC2::VPNGateway	예	예	예	예	예	예	예	예
AWS::EC2::Volume	예	예	예	예	예	예	예	예
AWS::ECR::PublicRepository	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::ECR::PullThroughCacheRule	예	예	예	예	예	예	아니요	예
AWS::ECR::RegistryPolicy	예	예	예	예	예	예	아니요	예
AWS::ECR::Repository	예	예	예	예	예	예	아니요	예
AWS::ECS::CapacityProvider	예	예	예	예	예	예	아니요	예
AWS::ECS::Cluster	예	예	예	예	예	예	예	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::ECS::Service	예	예	예	예	예	예	예	예
AWS::ECS::TaskDefinition	예	예	예	예	예	예	예	예
AWS::ECS::TaskSet	예	예	예	예	아니요	예	아니요	예
AWS::EFS::AccessPoint	예	예	예	예	예	예	아니요	예
AWS::EFS::FileSystem	예	예	예	예	예	예	아니요	예
AWS::EKS::Addon	예	예	예	예	아니요	예	아니요	예
AWS::EKS::Cluster	예	예	예	예	아니요	예	아니요	예
AWS::EKS::FargateProfile	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::EKS::Identity ProviderConfig	예	예	예	예	아니요	예	아니요	예
AWS::EMR::Security Configuration	예	예	예	예	예	예	아니요	예
AWS::ElasticBeanstalk::Application	예	예	예	예	아니요	예	아니요	예
AWS::ElasticBeanstalk::ApplicationVersion	예	예	예	예	아니요	예	아니요	예
AWS::ElasticBeanstalk::Environment	예	예	예	예	아니요	예	아니요	예
AWS::ElasticLoadBalancing::LoadBalancer	예	예	예	예	예	예	예	예
AWS::ElasticLoadBalancingV2::Listener	예	예	예	예	아니요	예	아니요	예
AWS::ElasticLoadBalancingV2::LoadBalancer	예	예	예	예	예	예	예	예
AWS::Elasticsearch::Domain	예	예	예	예	예	예	예	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::EventSchemas::Discoverer	예	예	예	예	아니요	예	아니요	예
AWS::EventSchemas::Registry	예	예	예	예	아니요	예	아니요	예
AWS::EventSchemas::RegistryPolicy	예	예	예	예	아니요	예	아니요	예
AWS::EventSchemas::Schema	예	예	예	예	아니요	예	아니요	예
AWS::Events::ApiDestination	예	예	예	예	아니요	예	아니요	예
AWS::Events::Archive	예	예	예	예	아니요	예	아니요	예
AWS::Events::Connection	예	예	예	예	아니요	예	아니요	예
AWS::Events::Endpoint	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::Events::EventBus	예	예	예	예	예	예	아니요	예
AWS::Events::Rule	예	예	예	예	아니요	예	아니요	예
AWS::Evidently::Launch	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::Evidently::Project	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::Evidently::Segment	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::FIS::ExperimentTemplate	예	예	예	예	아니요	예	아니요	예
AWS::Forecast::Dataset	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::Forecast::DatasetGroup	아니요	예	예	예	아니요	아니요	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::FraudDetector::EntityType	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::FraudDetector::Label	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::FraudDetector::Outcome	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::FraudDetector::Variable	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::GlobalAccelerator::Accelerator	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::GlobalAccelerator::EndpointGroup	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::GlobalAccelerator::Listener	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::Glue::Classifier	예	예	예	예	예	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::Glue::Job	예	예	예	예	예	예	아니요	예
AWS::Glue::MLTransform	예	예	예	예	예	예	아니요	예
AWS::Grafana::Workspace	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::GreengrassV2::ComponentVersion	아니요	예	예	예	아니요	예	아니요	아니요
AWS::GroundStation::Config	아니요	예	예	예	아니요	아니요	아니요	예
AWS::GroundStation::DataflowEndpointGroup	아니요	예	예	예	아니요	아니요	아니요	예
AWS::GroundStation::MissionProfile	아니요	예	예	예	아니요	아니요	아니요	예
AWS::GuardDuty::Detector	예	예	예	예	예	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::GuardDuty::Filter	예	예	예	예	아니요	예	아니요	예
AWS::GuardDuty::IPSet	예	예	예	예	아니요	예	아니요	예
AWS::GuardDuty::ThreatIntelSet	예	예	예	예	아니요	예	아니요	예
AWS::HealthLake::FHIRDatastore	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::IAM::Group	예	예	예	예	아니요	예	아니요	예
AWS::IAM::InstanceProfile	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IAM::OIDCProvider	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IAM::Policy	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::IAM::Role	예	예	예	예	아니요	예	아니요	예
AWS::IAM::SAMLProvider	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IAM::ServerCertificate	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IAM::User	예	예	예	예	아니요	예	아니요	예
AWS::IVS::Channel	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::IVS::PlaybackKeyPair	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::IVS::RecordingConfiguration	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::ImageBuilder::ContainerRecipe	예	예	예	예	예	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::ImageBuilder::DistributionConfiguration	예	예	예	예	예	예	아니요	예
AWS::ImageBuilder::ImagePipeline	예	예	예	예	예	예	아니요	예
AWS::ImageBuilder::ImageRecipe	예	예	예	예	예	예	아니요	예
AWS::ImageBuilder::InfrastructureConfiguration	예	예	예	예	아니요	예	아니요	예
AWS::InspectorV2::Activation	예	예	예	예	아니요	예	아니요	예
AWS::InspectorV2::Filter	예	예	예	예	아니요	예	아니요	예
AWS::IoT::AccountAuditConfiguration	예	예	예	예	아니요	예	아니요	아니요
AWS::IoT::Authorizer	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::IoT::CACertificate	예	예	예	예	아니요	예	아니요	예
AWS::IoT::CustomMetric	예	예	예	예	아니요	예	아니요	아니요
AWS::IoT::Dimension	예	예	예	예	아니요	예	아니요	아니요
AWS::IoT::FleetMetric	예	예	예	예	아니요	예	아니요	예
AWS::IoT::JobTemplate	예	예	예	예	아니요	예	아니요	예
AWS::IoT::MitigationAction	예	예	예	예	아니요	예	아니요	아니요
AWS::IoT::Policy	예	예	예	예	아니요	예	아니요	예
AWS::IoT::ProvisioningTemplate	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::IoT::RoleAlias	예	예	예	예	아니요	예	아니요	예
AWS::IoT::ScheduledAudit	예	예	예	예	아니요	예	아니요	아니요
AWS::IoT::SecurityProfile	예	예	예	예	아니요	예	아니요	아니요
AWS::IoTAnalytics::Channel	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::IoTAnalytics::Dataset	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::IoTAnalytics::Datastore	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::IoTAnalytics::Pipeline	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::IoTEvents::AlarmModel	아니요	예	예	예	아니요	예	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::IoTEvents::DetectorModel	아니요	예	예	예	아니요	예	아니요	아니요
AWS::IoTEvents::Input	아니요	예	예	예	아니요	예	아니요	아니요
AWS::IoTSiteWise::AssetModel	아니요	예	예	예	아니요	예	아니요	아니요
AWS::IoTSiteWise::Dashboard	아니요	예	예	예	아니요	예	아니요	아니요
AWS::IoTSiteWise::Gateway	아니요	예	예	예	아니요	예	아니요	아니요
AWS::IoTSiteWise::Portal	아니요	예	예	예	아니요	예	아니요	아니요
AWS::IoTSiteWise::Project	아니요	예	예	예	아니요	예	아니요	아니요
AWS::IoTTwinMaker::ComponentType	아니요	예	예	아니요	아니요	아니요	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::IoTTwinMaker::Entity	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::IoTTwinMaker::Scene	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::IoTTwinMaker::SyncJob	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::IoTTwinMaker::Workspace	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::IoTWireless::FuotaTask	아니요	예	예	아니요	아니요	아니요	아니요	예
AWS::IoTWireless::MulticastGroup	아니요	예	예	아니요	아니요	아니요	아니요	예
AWS::IoTWireless::ServiceProfile	아니요	예	예	아니요	아니요	아니요	아니요	예
AWS::KMS::Alias	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::KMS::Key	예	예	예	예	예	예	예	예
AWS::KafkaConnect::Connector	예	예	예	예	아니요	예	아니요	예
AWS::Kendra::Index	아니요	예	예	예	아니요	예	아니요	아니요
AWS::Kinesis::Stream	예	예	예	예	아니요	예	아니요	예
AWS::Kinesis::StreamConsumer	예	예	예	예	아니요	예	아니요	예
AWS::KinesisAnalyticsV2::Application	예	예	예	예	예	예	아니요	예
AWS::KinesisFirehose::DeliveryStream	예	예	예	예	아니요	예	아니요	예
AWS::KinesisVideo::SignalingChannel	아니요	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::KinesisVideo::Stream	아니요	예	예	예	아니요	예	아니요	예
AWS::Lambda::CodeSigningConfig	예	예	예	예	아니요	예	아니요	예
AWS::Lambda::Function	예	예	예	예	예	예	예	예
AWS::Lex::Bot	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::Lex::BotAlias	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::Lightsail::Bucket	아니요	예	예	예	아니요	예	아니요	아니요
AWS::Lightsail::Certificate	아니요	예	예	예	아니요	예	아니요	아니요
AWS::Lightsail::Disk	아니요	예	예	예	아니요	예	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::Lightsail::StaticIp	아니요	예	예	예	아니요	예	아니요	아니요
AWS::Logs::Destination	예	예	예	예	예	예	아니요	예
AWS::LookoutMetrics::Alert	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::LookoutVision::Project	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::M2::Environment	예	예	예	예	아니요	예	아니요	예
AWS::MSK::BatchScramSecret	예	예	예	예	아니요	예	아니요	예
AWS::MSK::Cluster	예	예	예	예	아니요	예	아니요	예
AWS::MSK::ClusterPolicy	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::MSK::Configuration	예	예	예	예	예	예	아니요	예
AWS::MSK::VpcConnection	예	예	예	예	아니요	예	아니요	예
AWS::Macie::Session	예	예	예	예	아니요	예	아니요	예
AWS::MediaConnect::FlowEntitlement	예	예	예	예	아니요	예	아니요	예
AWS::MediaConnect::FlowSource	예	예	예	예	아니요	예	아니요	예
AWS::MediaConnect::FlowVpcInterface	예	예	예	예	아니요	예	아니요	예
AWS::MediaConnect::Gateway	예	예	예	예	아니요	예	아니요	예
AWS::MediaPackage::PackagingConfiguration	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::MediaPackage::PackagingGroup	예	예	예	예	아니요	예	아니요	예
AWS::MediaTailor::PlaybackConfiguration	아니요	예	예	예	아니요	예	아니요	예
AWS::MemoryDB::SubnetGroup	예	예	예	예	아니요	예	아니요	예
AWS::NetworkFirewall::Firewall	예	예	예	예	예	예	예	예
AWS::NetworkFirewall::FirewallPolicy	예	예	예	예	예	예	예	예
AWS::NetworkFirewall::RuleGroup	예	예	예	예	예	예	예	예
AWS::NetworkFirewall::TLSInspectionConfiguration	예	예	예	예	예	예	예	예
AWS::NetworkFirewall::VpcEndpointAssociation	예	예	예	예	예	예	예	예
AWS::NetworkManager::ConnectPeer	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::NetworkManager::CustomerGatewayAssociation	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::NetworkManager::Device	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::NetworkManager::GlobalNetwork	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::NetworkManager::Link	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::NetworkManager::LinkAssociation	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::NetworkManager::Site	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::NetworkManager::TransitGatewayRegistration	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::OpenSearch::Domain	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::OpenSearchServerless::Collection	아니요	예	예	예	아니요	예	아니요	예
AWS::OpenSearchServerless::VpcEndpoint	아니요	예	예	예	아니요	예	아니요	예
AWS::Panorama::Package	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::Personalize::Dataset	아니요	예	예	예	아니요	예	아니요	아니요
AWS::Personalize::DatasetGroup	아니요	예	예	예	아니요	예	아니요	아니요
AWS::Personalize::Schema	아니요	예	예	예	아니요	예	아니요	아니요
AWS::Personalize::Solution	아니요	예	예	예	아니요	예	아니요	아니요
AWS::Pinpoint::App	아니요	예	예	아니요	아니요	예	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::Pinpoint::ApplicationSettings	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::Pinpoint::Campaign	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::Pinpoint::EmailChannel	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::Pinpoint::EmailTemplate	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::Pinpoint::EventStream	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::Pinpoint::InAppTemplate	아니요	예	예	예	아니요	예	아니요	아니요
AWS::Pinpoint::Segment	아니요	예	예	아니요	아니요	예	아니요	아니요
AWS::QLDB::Ledger	아니요	예	예	예	아니요	예	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::QuickSight::DataSource	아니요	예	예	예	아니요	예	아니요	예
AWS::QuickSight::Template	아니요	예	예	예	아니요	예	아니요	예
AWS::QuickSight::Theme	아니요	예	예	예	아니요	예	아니요	예
AWS::RDS::DBCluster	예	예	예	예	예	예	예	예
AWS::RDS::DBClusterSnapshot	예	예	예	예	예	예	예	예
AWS::RDS::DBInstance	예	예	예	예	예	예	예	예
AWS::RDS::DBSecurityGroup	예	예	예	예	예	예	예	예
AWS::RDS::DBSnapshot	예	예	예	예	예	예	예	예
AWS::RDS::DBSubnetGroup	예	예	예	예	예	예	예	예
AWS::RDS::EventSubscription	예	예	예	예	예	예	예	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::RDS::GlobalCluster	예	예	예	예	아니요	예	아니요	예
AWS::RDS::OptionGroup	예	예	예	예	예	예	아니요	예
AWS::RUM::AppMonitor	예	예	예	예	아니요	예	아니요	예
AWS::Redshift::Cluster	예	예	예	예	예	예	예	예
AWS::Redshift::ClusterParameterGroup	예	예	예	예	예	예	예	예
AWS::Redshift::ClusterSecurityGroup	예	예	예	예	예	예	예	예
AWS::Redshift::ClusterSnapshot	예	예	예	예	예	예	예	예
AWS::Redshift::ClusterSubnetGroup	예	예	예	예	예	예	예	예
AWS::Redshift::EndpointAccess	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::Redshift::EndpointAuthorization	예	예	예	예	아니요	예	아니요	예
AWS::Redshift::EventSubscription	예	예	예	예	예	예	예	예
AWS::Redshift::ScheduledAction	예	예	예	예	아니요	예	아니요	예
AWS::ResilienceHub::App	예	예	예	예	아니요	예	아니요	예
AWS::ResilienceHub::ResiliencyPolicy	예	예	예	예	아니요	예	아니요	예
AWS::ResourceExplorer2::Index	예	예	예	예	예	예	아니요	예
AWS::RoboMaker::RobotApplication	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::RoboMaker::RobotApplicationVersion	아니요	예	예	예	아니요	아니요	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::RoboMaker::SimulationApplication	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::Route53::HealthCheck	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::Route53::HostedZone	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::Route53Profiles::Profile	예	예	예	예	예	예	아니요	예
AWS::Route53RecoveryControl::Cluster	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::Route53RecoveryControl::ControlPanel	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::Route53RecoveryControl::RoutingControl	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::Route53RecoveryControl::SafetyRule	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::Route53RecoveryReadiness::Cell	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::Route53RecoveryReadiness::ReadinessCheck	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::Route53RecoveryReadiness::RecoveryGroup	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::Route53RecoveryReadiness::ResourceSet	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::Route53Resolver::FirewallDomainList	예	예	예	예	아니요	예	아니요	예
AWS::Route53Resolver::FirewallRuleGroup	예	예	예	예	아니요	예	아니요	예
AWS::Route53Resolver::FirewallRuleGroupAssociation	예	예	예	예	아니요	예	아니요	예
AWS::Route53Resolver::ResolverEndpoint	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::Route53Resolver::ResolverQueryLoggingConfig	예	예	예	예	아니요	예	아니요	예
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	예	예	예	예	아니요	예	아니요	예
AWS::Route53Resolver::ResolverRule	예	예	예	예	아니요	예	아니요	예
AWS::Route53Resolver::ResolverRuleAssociation	예	예	예	예	아니요	예	아니요	예
AWS::S3::AccessPoint	예	예	예	예	아니요	예	아니요	예
AWS::S3::AccountPublicAccessBlock	예	예	예	예	아니요	예	아니요	예
AWS::S3::Bucket	예	예	예	예	예	예	예	예
AWS::S3::MultiRegionAccessPoint	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::S3::StorageLens	예	예	예	예	아니요	예	아니요	예
AWS::S3::StorageLensGroup	예	예	예	예	아니요	예	아니요	예
AWS::S3Express::BucketPolicy	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::S3Express::DirectoryBucket	아니요	예	예	예	아니요	아니요	아니요	아니요
AWS::SES::ConfigurationSet	예	예	예	예	아니요	예	아니요	예
AWS::SES::ContactList	예	예	예	예	아니요	예	아니요	예
AWS::SES::ReceiptFilter	아니요	예	예	예	아니요	예	아니요	아니요
AWS::SES::ReceiptRuleSet	아니요	예	예	예	아니요	예	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::SES::Template	예	예	예	예	아니요	예	아니요	예
AWS::SNS::Topic	예	예	예	예	예	예	예	예
AWS::SQS::Queue	예	예	예	예	아니요	예	아니요	예
AWS::SSM::AssociationCompliance	예	예	예	예	예	예	예	예
AWS::SSM::Document	예	예	예	예	예	예	아니요	예
AWS::SSM::FileData	예	예	예	예	예	예	예	예
AWS::SSM::ManagedInstanceInventory	예	예	예	예	예	예	예	예
AWS::SSM::PatchCompliance	예	예	예	예	예	예	예	예
AWS::SageMaker::AppImageConfig	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::SageMaker::CodeRepository	예	예	예	예	아니요	예	아니요	예
AWS::SageMaker::Domain	예	예	예	예	아니요	예	아니요	예
AWS::SageMaker::EndpointConfig	예	예	예	예	아니요	예	아니요	예
AWS::SageMaker::FeatureGroup	예	예	예	예	아니요	예	아니요	예
AWS::SageMaker::Image	예	예	예	예	아니요	예	아니요	예
AWS::SageMaker::InferenceExperiment	예	예	예	예	아니요	예	아니요	예
AWS::SageMaker::Model	예	예	예	예	아니요	예	아니요	예
AWS::SageMaker::NotebookInstance	예	예	예	예	아니요	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::SageMaker::NotebookInstanceLifecycleConfig	예	예	예	예	아니요	예	아니요	예
AWS::SageMaker::Workteam	아니요	예	예	예	아니요	예	아니요	아니요
AWS::SecretsManager::Secret	예	예	예	예	예	예	예	예
AWS::SecurityHub::Standard	예	예	예	예	예	예	예	예
AWS::ServiceCatalog::CloudFormationProduct	예	예	예	예	아니요	예	아니요	예
AWS::ServiceCatalog::CloudFormationProvisionedProduct	예	예	예	예	아니요	예	아니요	예
AWS::ServiceCatalog::Portfolio	예	예	예	예	아니요	예	아니요	예
AWS::ServiceDiscovery::HttpNamespace	예	예	예	예	예	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::ServiceDiscovery::Instance	예	예	예	예	아니요	예	아니요	예
AWS::ServiceDiscovery::PublicDnsNamespace	예	예	예	예	예	예	아니요	예
AWS::ServiceDiscovery::Service	예	예	예	예	아니요	예	아니요	예
AWS::Shield::Protection	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::ShieldRegional::Protection	예	예	예	예	아니요	예	아니요	예
AWS::Signer::SigningProfile	예	예	예	예	아니요	예	아니요	예
AWS::StepFunctions::Activity	예	예	예	예	예	예	아니요	예
AWS::StepFunctions::StateMachine	예	예	예	예	예	예	아니요	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::Transfer::Agreement	예	예	예	예	아니요	예	아니요	예
AWS::Transfer::Certificate	예	예	예	예	예	예	아니요	예
AWS::Transfer::Connector	예	예	예	예	예	예	아니요	예
AWS::Transfer::Profile	예	예	예	예	예	예	아니요	예
AWS::Transfer::Workflow	예	예	예	예	예	예	아니요	예
AWS::WAF::RateBasedRule	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::WAF::Rule	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::WAF::RuleGroup	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::WAF::WebACL	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::WAFRegional::RateBasedRule	예	예	예	예	아니요	예	아니요	예
AWS::WAFRegional::Rule	예	예	예	예	아니요	예	아니요	예
AWS::WAFRegional::RuleGroup	예	예	예	예	아니요	예	아니요	예
AWS::WAFRegional::WebACL	예	예	예	예	아니요	예	아니요	예
AWS::WAFv2::IPSet	예	예	예	예	예	예	예	예
AWS::WAFv2::ManagedRuleSet	예	예	예	예	예	예	예	예
AWS::WAFv2::RegexPatternSet	예	예	예	예	예	예	예	예
AWS::WAFv2::RuleGroup	예	예	예	예	예	예	예	예

리소스 유형	미국 서부 (캘리포니아 북부)	미국 동부 (버지니아 북부)	미국 서부 (오리건)	미국 동부 (오하이오)	캐나다 서부 (캘거리)	캐나다(중부)	멕시코 (중부)	남아메리카 (상파울루)
AWS::WAFv2::WebACL	예	예	예	예	예	예	예	예
AWS::WorkSpaces::ConnectionAlias	아니요	예	예	아니요	아니요	예	아니요	예
AWS::WorkSpaces::Workspace	아니요	예	예	아니요	아니요	예	아니요	예
AWS::XRay::EncryptionConfig	예	예	예	예	아니요	예	아니요	예

유럽 리전

리소스 유형	유럽 (아일랜드)	유럽 (프랑크푸르트)	유럽 (런던)	유럽 (파리)	유럽 (스톡홀름)	유럽 (밀라노)	유럽 (스페인)	유럽 (취리히)
AWS::ACM::Certificate	예	예	예	예	예	예	예	예
AWS::ACMPCA::CertificateAuthority	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::ACMPCA::CertificateAuthorityActivation	예	예	예	예	예	예	예	예
AWS::APS::RuleGroupsNamespace	예	예	예	예	예	아니요	아니요	아니요
AWS::AccessAnalyzer::Analyzer	예	예	예	예	예	예	예	예
AWS::AmazonMQ::Broker	예	예	예	예	예	예	아니요	아니요
AWS::Amplify::App	예	예	예	예	예	예	아니요	아니요
AWS::Amplify::Branch	예	예	예	예	예	예	아니요	아니요
AWS::ApiGateway::RestApi	예	예	예	예	예	예	예	예
AWS::ApiGateway::Stage	예	예	예	예	예	예	예	예
AWS::ApiGatewayV2::Api	예	예	예	예	예	예	예	예
AWS::ApiGatewayV2::Stage	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::AppConfig::Application	예	예	예	예	예	예	아니요	아니요
AWS::AppConfig::ConfigurationProfile	예	예	예	예	예	예	아니요	아니요
AWS::AppConfig::DeploymentStrategy	예	예	예	예	예	예	예	예
AWS::AppConfig::Environment	예	예	예	예	예	예	아니요	아니요
AWS::AppConfig::ExtensionAssociation	예	예	예	예	예	예	예	예
AWS::AppConfig::HostedConfigurationVersion	예	예	예	예	예	예	아니요	아니요
AWS::AppFlow::Flow	예	예	예	예	아니요	아니요	아니요	아니요
AWS::AppIntegrations::Application	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::AppIntegrations::EventIntegration	아니요	예	예	아니요	아니요	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::AppMesh::GatewayRoute	예	예	예	예	예	예	아니요	아니요
AWS::AppMesh::Mesh	예	예	예	예	예	예	아니요	아니요
AWS::AppMesh::Route	예	예	예	예	예	예	아니요	아니요
AWS::AppMesh::VirtualGateway	예	예	예	예	예	예	아니요	아니요
AWS::AppMesh::VirtualNode	예	예	예	예	예	예	아니요	아니요
AWS::AppMesh::VirtualRouter	예	예	예	예	예	예	아니요	아니요
AWS::AppMesh::VirtualService	예	예	예	예	예	예	아니요	아니요
AWS::AppRunner::Service	예	예	예	예	아니요	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::AppRunner::VpcConnector	예	예	아니요	예	아니요	아니요	아니요	아니요
AWS::AppStream::Application	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::AppStream::DirectoryConfig	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::AppStream::Fleet	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::AppStream::Stack	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::AppSync::ApiCache	예	예	예	예	예	예	예	예
AWS::AppSync::GraphQLApi	예	예	예	예	예	예	예	예
AWS::Athena::DataCatalog	예	예	예	예	예	예	예	예
AWS::Athena::PreparedStatement	예	예	예	예	예	아니요	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::Athena::WorkGroup	예	예	예	예	예	예	예	예
AWS::AuditManager::Assessment	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::AutoScaling::AutoScalingGroup	예	예	예	예	예	예	예	예
AWS::AutoScaling::LaunchConfiguration	예	예	예	예	예	예	예	예
AWS::AutoScaling::ScalingPolicy	예	예	예	예	예	예	예	예
AWS::AutoScaling::ScheduledAction	예	예	예	예	예	예	예	예
AWS::Auto Scaling::WarmPool	예	예	예	예	예	예	아니요	아니요
AWS::Backup::BackupPlan	예	예	예	예	예	예	예	예
AWS::Back up::BackupSelection	예	예	예	예	예	예	예	예
AWS::Backup::BackupVault	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::Backup::RecoveryPoint	예	예	예	예	예	예	예	예
AWS::Backup::ReportPlan	예	예	예	예	예	예	아니요	아니요
AWS::Batch::ComputeEnvironment	예	예	예	예	예	예	예	예
AWS::Batch::JobQueue	예	예	예	예	예	예	예	예
AWS::Batch::SchedulingPolicy	예	예	예	예	예	예	예	예
AWS::Bedrock::Guardrail	예	예	예	예	예	예	예	예
AWS::Bedrock::KnowledgeBase	예	예	예	예	예	아니요	아니요	예
AWS::Cassandra::Keyspace	예	예	예	예	예	아니요	아니요	아니요
AWS::Cloud9::EnvironmentEC2	예	예	예	예	예	예	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::CloudFormation::Stack	예	예	예	예	예	예	아니요	아니요
AWS::CloudTrail::Trail	예	예	예	예	예	예	예	예
AWS::CloudWatch::Alarm	예	예	예	예	예	예	예	예
AWS::CloudWatch::MetricStream	예	예	예	예	예	예	예	예
AWS::CodeArtifact::Repository	예	예	예	예	예	예	아니요	아니요
AWS::CodeBuild::Project	예	예	예	예	예	예	예	예
AWS::CodeBuild::ReportGroup	예	예	예	예	예	예	예	예
AWS::CodeDeploy::Application	예	예	예	예	예	예	아니요	아니요
AWS::CodeDeploy::DeploymentConfig	예	예	예	예	예	예	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::CodeDeploy::DeploymentGroup	예	예	예	예	예	예	아니요	아니요
AWS::CodeGuruProfiler::ProfilingGroup	예	예	예	아니요	예	아니요	아니요	아니요
AWS::CodeGuruReviewer::RepositoryAssociation	예	예	예	아니요	예	아니요	아니요	아니요
AWS::CodePipeline::Pipeline	예	예	예	예	예	예	예	예
AWS::Cognito::IdentityPool	예	예	예	예	예	예	예	예
AWS::Cognito::UserPool	예	예	예	예	예	예	예	예
AWS::Cognito::UserPoolClient	예	예	예	예	예	예	예	예
AWS::Cognito::UserPoolGroup	예	예	예	예	예	예	예	예
AWS::Config::ConfigurationRecorder	예	예	예	예	예	예	예	예
AWS::Config::ConformancePackCompliance	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::Config::ResourceCompliance	예	예	예	예	예	예	예	예
AWS::Connect::Instance	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Connect::PhoneNumber	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Connect::QuickConnect	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Connect::Rule	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Connect::User	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::CustomerProfiles::Domain	아니요	예	예	아니요	아니요	아니요	아니요	아니요
AWS::CustomerProfiles::ObjectType	아니요	예	예	아니요	아니요	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::DMS::Certificate	예	예	예	예	예	예	아니요	아니요
AWS::DMS::Endpoint	예	예	예	예	예	예	아니요	아니요
AWS::DMS::EventSubscription	예	예	예	예	예	예	아니요	아니요
AWS::DMS::ReplicationInstance	예	예	예	예	예	예	아니요	아니요
AWS::DMS::ReplicationSubnetGroup	예	예	예	예	예	예	아니요	아니요
AWS::DMS::ReplicationTask	예	예	예	예	예	예	아니요	아니요
AWS::DataSync::LocationEFS	예	예	예	예	예	예	예	예
AWS::DataSync::LocationFSxLustre	예	예	예	예	예	예	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::DataSync::LocationFSxWindows	예	예	예	예	예	예	아니요	아니요
AWS::DataSync::LocationHDFS	예	예	예	예	예	예	예	예
AWS::DataSync::LocationNFS	예	예	예	예	예	예	예	예
AWS::DataSync::LocationObjectStorage	예	예	예	예	예	예	예	예
AWS::DataSync::LocationS3	예	예	예	예	예	예	예	예
AWS::DataSync::LocationSMB	예	예	예	예	예	예	예	예
AWS::DataSync::Task	예	예	예	예	예	예	예	예
AWS::Detective::Graph	예	예	예	예	예	예	아니요	아니요
AWS::DynamoDB::Table	예	예	예	예	예	예	예	예
AWS::EC2::CapacityReservation	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::EC2::CarrierGateway	예	예	예	예	아니요	아니요	아니요	아니요
AWS::EC2::ClientVpnEndpoint	예	예	예	예	예	예	아니요	예
AWS::EC2::ClientVpnTargetNetworkAssociation	예	예	예	예	예	예	아니요	예
AWS::EC2::CustomerGateway	예	예	예	예	예	예	예	예
AWS::EC2::DHCPOptions	예	예	예	예	예	예	예	예
AWS::EC2::EC2Fleet	예	예	예	예	예	예	예	예
AWS::EC2::EIP	예	예	예	예	예	예	예	예
AWS::EC2::EIPAssociation	예	예	예	예	예	예	예	예
AWS::EC2::EgressOnlyInternetGateway	예	예	예	예	예	예	아니요	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::EC2::FlowLog	예	예	예	예	예	예	아니요	예
AWS::EC2::Host	예	예	예	예	예	예	예	예
AWS::EC2::IPAM	예	예	예	예	예	예	예	예
AWS::EC2::IPAMPool	예	예	예	예	예	예	예	예
AWS::EC2::IPAMResourceDiscovery	예	예	예	예	예	예	예	예
AWS::EC2::IPAMResourceDiscoveryAssociation	예	예	예	예	예	예	예	예
AWS::EC2::IPAMScope	예	예	예	예	예	예	예	예
AWS::EC2::Instance	예	예	예	예	예	예	예	예
AWS::EC2::InstanceConnectEndpoint	예	예	예	예	예	예	예	예
AWS::EC2::InternetGateway	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::EC2::LaunchTemplate	예	예	예	예	예	예	아니요	아니요
AWS::EC2::NatGateway	예	예	예	예	예	예	아니요	예
AWS::EC2::NetworkAcl	예	예	예	예	예	예	예	예
AWS::EC2::NetworkInsightsAccessScope	예	예	예	예	예	예	아니요	아니요
AWS::EC2::NetworkInsightsAccessScopeAnalysis	예	예	예	예	예	예	아니요	아니요
AWS::EC2::NetworkInsightsAnalysis	예	예	예	예	예	예	아니요	아니요
AWS::EC2::NetworkInsightsPath	예	예	예	예	예	예	아니요	아니요
AWS::EC2::NetworkInterface	예	예	예	예	예	예	예	예
AWS::EC2::PrefixList	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::EC2::RegisteredHAInstance	예	예	예	예	예	아니요	아니요	아니요
AWS::EC2::RouteTable	예	예	예	예	예	예	예	예
AWS::EC2::SecurityGroup	예	예	예	예	예	예	예	예
AWS::EC2::SnapshotBlockPublicAccess	예	예	예	예	예	예	예	예
AWS::EC2::SpotFleet	예	예	예	예	예	예	예	예
AWS::EC2::Subnet	예	예	예	예	예	예	예	예
AWS::EC2::SubnetRouteTableAssociation	예	예	예	예	예	예	예	예
AWS::EC2::TrafficMirrorFilter	예	예	예	예	예	예	예	예
AWS::EC2::TrafficMirrorSession	예	예	예	예	예	아니요	아니요	예
AWS::EC2::TrafficMirrorTarget	예	예	예	예	예	예	아니요	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::EC2::TransitGateway	예	예	예	예	예	예	예	예
AWS::EC2::TransitGatewayAttachment	예	예	예	예	예	예	예	예
AWS::EC2::TransitGatewayConnect	예	예	예	예	예	예	아니요	예
AWS::EC2::TransitGatewayMulticastDomain	예	예	예	예	예	예	예	예
AWS::EC2::TransitGatewayRouteTable	예	예	예	예	예	예	아니요	예
AWS::EC2::VPC	예	예	예	예	예	예	예	예
AWS::EC2::VPCBlockPublicAccessExclusion	예	예	예	예	예	예	예	예
AWS::EC2::VPCBlockPublicAccessOptions	예	예	예	예	예	예	예	예
AWS::EC2::VPCEndpoint	예	예	예	예	예	예	예	예
AWS::EC2::VPCEndpointConnectionNotification	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::EC2::VPCEndpointService	예	예	예	예	예	예	예	예
AWS::EC2::VPCPeeringConnection	예	예	예	예	예	예	예	예
AWS::EC2::VPNConnection	예	예	예	예	예	예	예	예
AWS::EC2::VPNConnectionRoute	예	예	예	예	예	예	예	예
AWS::EC2::VPNGateway	예	예	예	예	예	예	예	예
AWS::EC2::Volume	예	예	예	예	예	예	예	예
AWS::ECR::PullThroughCacheRule	예	예	예	예	예	예	예	예
AWS::ECR::RegistryPolicy	예	예	예	예	예	예	예	예
AWS::ECR::Repository	예	예	예	예	예	예	예	예
AWS::ECS::CapacityProvider	예	예	예	예	예	예	예	예
AWS::ECS::Cluster	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::ECS::Service	예	예	예	예	예	예	예	예
AWS::ECS::TaskDefinition	예	예	예	예	예	예	예	예
AWS::ECS::TaskSet	예	예	예	예	예	예	예	예
AWS::EFS::AccessPoint	예	예	예	예	예	예	예	예
AWS::EFS::FileSystem	예	예	예	예	예	예	예	예
AWS::EKS::Addon	예	예	예	예	예	예	예	예
AWS::EKS::Cluster	예	예	예	예	예	예	예	예
AWS::EKS::FargateProfile	예	예	예	예	예	예	예	예
AWS::EKS::IdentityProviderConfig	예	예	예	예	예	예	예	예
AWS::EMR::SecurityConfiguration	예	예	예	예	예	예	예	예
AWS::ElasticBeanstalk::Application	예	예	예	예	예	예	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::ElasticBeanstalk::ApplicationVersion	예	예	예	예	예	예	아니요	아니요
AWS::ElasticBeanstalk::Environment	예	예	예	예	예	예	아니요	아니요
AWS::ElasticLoadBalancing::LoadBalancer	예	예	예	예	예	예	예	예
AWS::ElasticLoadBalancingV2::Listener	예	예	예	예	예	예	아니요	아니요
AWS::ElasticLoadBalancingV2::LoadBalancer	예	예	예	예	예	예	예	예
AWS::Elasticsearch::Domain	예	예	예	예	예	예	예	예
AWS::EventSchemas::Discoverer	예	예	예	예	예	예	예	예
AWS::EventSchemas::Registry	예	예	예	예	예	예	예	예
AWS::EventSchemas::RegistryPolicy	예	예	예	예	예	예	예	예
AWS::EventSchemas::Schema	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::Events::ApiDestination	예	예	예	예	예	예	예	예
AWS::Events::Archive	예	예	예	예	예	예	예	예
AWS::Events::Connection	예	예	예	예	예	예	예	예
AWS::Events::Endpoint	예	예	예	예	예	아니요	아니요	아니요
AWS::Events::EventBus	예	예	예	예	예	예	예	예
AWS::Events::Rule	예	예	예	예	예	예	예	예
AWS::Evidently::Launch	예	예	아니요	아니요	예	아니요	아니요	아니요
AWS::Evidently::Project	예	예	아니요	아니요	예	아니요	아니요	아니요
AWS::Evidently::Segment	예	예	아니요	아니요	예	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::FIS::ExperimentTemplate	예	예	예	예	예	예	예	아니요
AWS::Forecast::Dataset	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::Forecast::DatasetGroup	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::FraudDetector::EntityType	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
AWS::FraudDetector::Label	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
AWS::FraudDetector::Outcome	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
AWS::FraudDetector::Variable	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
AWS::Glue::Classifier	예	예	예	예	예	예	예	예
AWS::Glue::Job	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::Glue::MLTransform	예	예	예	예	예	예	예	예
AWS::Grafana::Workspace	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::GreengrassV2::ComponentVersion	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::GroundStation::Config	예	예	아니요	아니요	예	아니요	아니요	아니요
AWS::GroundStation::DataflowEndpointGroup	예	예	아니요	아니요	예	아니요	아니요	아니요
AWS::GroundStation::MissionProfile	예	예	아니요	아니요	예	아니요	아니요	아니요
AWS::GuardDuty::Detector	예	예	예	예	예	예	예	예
AWS::GuardDuty::Filter	예	예	예	예	예	예	아니요	아니요
AWS::GuardDuty::IPSet	예	예	예	예	예	예	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::GuardDuty::ThreatIntelSet	예	예	예	예	예	예	예	예
AWS::IAM::Group	예	예	예	예	예	예	아니요	아니요
AWS::IAM::Policy	예	예	예	예	예	예	아니요	아니요
AWS::IAM::Role	예	예	예	예	예	예	아니요	아니요
AWS::IAM::User	예	예	예	예	예	예	아니요	아니요
AWS::IVS::Channel	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IVS::PlaybackKeyPair	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IVS::RecordingConfiguration	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::ImageBuilder::ContainerRecipe	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::ImageBuilder::DistributionConfiguration	예	예	예	예	예	예	예	예
AWS::ImageBuilder::ImagePipeline	예	예	예	예	예	예	예	예
AWS::ImageBuilder::ImageRecipe	예	예	예	예	예	예	예	예
AWS::ImageBuilder::InfrastructureConfiguration	예	예	예	예	예	예	예	예
AWS::InspectorV2::Activation	예	예	예	예	예	예	아니요	예
AWS::InspectorV2::Filter	예	예	예	예	예	예	아니요	예
AWS::IoT::AccountAuditConfiguration	예	예	예	예	예	아니요	아니요	아니요
AWS::IoT::Authorizer	예	예	예	예	예	아니요	아니요	아니요
AWS::IoT::CACertificate	예	예	예	예	예	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::IoT::CustomMetric	예	예	예	예	예	아니요	아니요	아니요
AWS::IoT::Dimension	예	예	예	예	예	아니요	아니요	아니요
AWS::IoT::FleetMetric	예	예	예	예	예	아니요	아니요	아니요
AWS::IoT::JobTemplate	예	예	예	예	예	아니요	아니요	아니요
AWS::IoT::MitigationAction	예	예	예	예	예	아니요	아니요	아니요
AWS::IoT::Policy	예	예	예	예	예	아니요	아니요	아니요
AWS::IoT::ProvisioningTemplate	예	예	예	예	예	아니요	아니요	아니요
AWS::IoT::RoleAlias	예	예	예	예	예	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::IoT::ScheduledAudit	예	예	예	예	예	아니요	아니요	아니요
AWS::IoT::SecurityProfile	예	예	예	예	예	아니요	아니요	아니요
AWS::IoTAnalytics::Channel	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTAnalytics::Dataset	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTAnalytics::Datastore	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTAnalytics::Pipeline	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTEvents::AlarmModel	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::IoTEvents::DetectorModel	예	예	예	아니요	아니요	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::IoTEvents::Input	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::IoTSiteWise::AssetModel	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTSiteWise::Dashboard	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTSiteWise::Gateway	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTSiteWise::Portal	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTSiteWise::Project	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTTwinMaker::ComponentType	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTTwinMaker::Entity	예	예	아니요	아니요	아니요	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::IoTTwinMaker::Scene	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTTwinMaker::SyncJob	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTTwinMaker::Workspace	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTWireless::FuotaTask	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTWireless::MulticastGroup	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IoTWireless::ServiceProfile	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::KMS::Alias	예	예	예	예	예	예	아니요	예
AWS::KMS::Key	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::KafkaConnect::Connector	예	예	예	예	예	아니요	아니요	아니요
AWS::Kendra::Index	예	아니요	예	아니요	아니요	아니요	아니요	아니요
AWS::Kinesis::Stream	예	예	예	예	예	예	예	예
AWS::Kinesis::StreamConsumer	예	예	예	예	예	예	예	예
AWS::KinesisAnalyticsV2::Application	예	예	예	예	예	예	예	예
AWS::KinesisFirehose::DeliveryStream	예	예	예	예	예	예	예	예
AWS::KinesisVideo::SignalingChannel	예	예	예	예	아니요	아니요	아니요	아니요
AWS::KinesisVideo::Stream	예	예	예	예	아니요	아니요	아니요	아니요
AWS::Lambda::CodeSigningConfig	예	예	예	예	예	예	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::Lambda::Function	예	예	예	예	예	예	예	예
AWS::Lex::Bot	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Lex::BotAlias	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Lightsail::Bucket	예	예	예	예	예	아니요	아니요	아니요
AWS::Lightsail::Certificate	예	예	예	예	예	아니요	아니요	아니요
AWS::Lightsail::Disk	예	예	예	예	예	아니요	아니요	아니요
AWS::Lightsail::StaticIp	예	예	예	예	예	아니요	아니요	아니요
AWS::Logs::Destination	예	예	예	예	예	예	예	예
AWS::LookoutMetrics::Alert	예	예	아니요	아니요	예	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::LookoutVision::Project	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::M2::Environment	예	예	예	예	예	예	아니요	아니요
AWS::MSK::BatchScramSecret	예	예	예	예	예	예	예	예
AWS::MSK::Cluster	예	예	예	예	예	예	예	예
AWS::MSK::ClusterPolicy	예	예	예	예	예	예	예	예
AWS::MSK::Configuration	예	예	예	예	예	예	예	예
AWS::MSK::VpcConnection	예	예	예	예	예	예	예	예
AWS::Macie::Session	예	예	예	예	예	예	아니요	아니요
AWS::MediaConnect::FlowEntitlement	예	예	예	예	예	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::MediaConnect::FlowSource	예	예	예	예	예	아니요	아니요	아니요
AWS::MediaConnect::FlowVpcInterface	예	예	예	예	예	아니요	아니요	아니요
AWS::MediaConnect::Gateway	예	예	예	예	예	아니요	아니요	아니요
AWS::MediaPackage::PackagingConfiguration	예	예	예	예	예	아니요	아니요	아니요
AWS::MediaPackage::PackagingGroup	예	예	예	예	예	아니요	아니요	아니요
AWS::MediaTailor::PlaybackConfiguration	예	예	아니요	예	예	아니요	아니요	아니요
AWS::MemoryDB::SubnetGroup	예	예	예	아니요	예	아니요	아니요	아니요
AWS::NetworkFirewall::Firewall	예	예	예	예	예	예	예	예
AWS::NetworkFirewall::FirewallPolicy	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::NetworkFirewall::RuleGroup	예	예	예	예	예	예	예	예
AWS::NetworkFirewall::TLSInspectionConfiguration	예	예	예	예	예	예	예	예
AWS::NetworkFirewall::VpcEndpointAssociation	예	예	예	예	예	예	예	예
AWS::OpenSearch::Domain	예	예	예	예	예	예	아니요	아니요
AWS::OpenSearchServerless::Collection	예	예	예	예	아니요	아니요	아니요	아니요
AWS::OpenSearchServerless::VpcEndpoint	예	예	예	예	아니요	아니요	아니요	아니요
AWS::Panorama::Package	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
AWS::Personalize::Dataset	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::Personalize::DatasetGroup	예	예	아니요	아니요	아니요	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::Personalize::Schema	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::Personalize::Solution	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::Pinpoint::App	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Pinpoint::ApplicationSettings	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Pinpoint::Campaign	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Pinpoint::EmailChannel	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Pinpoint::EmailTemplate	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Pinpoint::EventStream	예	예	예	아니요	아니요	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::Pinpoint::InAppTemplate	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::Pinpoint::Segment	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::QLDB::Ledger	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::QuickSight::DataSource	예	예	예	예	예	아니요	아니요	아니요
AWS::QuickSight::Template	예	예	예	예	예	아니요	아니요	아니요
AWS::QuickSight::Theme	예	예	예	예	예	아니요	아니요	아니요
AWS::RDS::DBCluster	예	예	예	예	예	예	예	예
AWS::RDS::DBClusterSnapshot	예	예	예	예	예	예	예	예
AWS::RDS::DBInstance	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::RDS::DBSecurityGroup	예	예	예	예	예	예	예	예
AWS::RDS::DBSnapshot	예	예	예	예	예	예	예	예
AWS::RDS::DBSubnetGroup	예	예	예	예	예	예	예	예
AWS::RDS::EventSubscription	예	예	예	예	예	예	예	예
AWS::RDS::GlobalCluster	예	예	예	예	예	예	예	예
AWS::RDS::OptionGroup	예	예	예	예	예	예	예	예
AWS::RUM::AppMonitor	예	예	예	예	예	예	예	예
AWS::Redshift::Cluster	예	예	예	예	예	예	예	예
AWS::Redshift::ClusterParameterGroup	예	예	예	예	예	예	예	예
AWS::Redshift::ClusterSecurityGroup	예	예	예	예	예	예	예	예
AWS::Redshift::ClusterSnapshot	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::Redshift::ClusterSubnetGroup	예	예	예	예	예	예	예	예
AWS::Redshift::EndpointAccess	예	예	예	예	예	아니요	아니요	아니요
AWS::Redshift::EndpointAuthorization	예	예	예	예	예	아니요	아니요	아니요
AWS::Redshift::EventSubscription	예	예	예	예	예	예	예	예
AWS::Redshift::ScheduledAction	예	예	예	예	예	예	아니요	아니요
AWS::ResilienceHub::App	예	예	예	예	예	예	아니요	아니요
AWS::ResilienceHub::ResiliencyPolicy	예	예	예	예	예	예	아니요	아니요
AWS::ResourceExplorer2::Index	예	예	예	예	예	예	예	예
AWS::RoboMaker::RobotApplication	예	예	아니요	아니요	아니요	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::RoboMaker::RobotApplicationVersion	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::RoboMaker::SimulationApplication	예	예	아니요	아니요	아니요	아니요	아니요	아니요
AWS::Route53Profiles::Profile	예	예	예	예	예	예	예	예
AWS::Route53Resolver::FirewallDomainList	예	예	예	예	예	예	아니요	아니요
AWS::Route53Resolver::FirewallRuleGroup	예	예	예	예	예	예	아니요	아니요
AWS::Route53Resolver::FirewallRuleGroupAssociation	예	예	예	예	예	예	아니요	아니요
AWS::Route53Resolver::ResolverEndpoint	예	예	예	예	예	예	예	예
AWS::Route53Resolver::ResolverQueryLoggingConfig	예	예	예	예	예	예	아니요	아니요
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	예	예	예	예	예	예	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::Route53Resolver::ResolverRule	예	예	예	예	예	예	예	예
AWS::Route53Resolver::ResolverRuleAssociation	예	예	예	예	예	예	예	예
AWS::S3::AccessPoint	예	예	예	예	예	예	예	예
AWS::S3::AccountPublicAccessBlock	예	예	예	예	예	예	예	예
AWS::S3::Bucket	예	예	예	예	예	예	예	예
AWS::S3::StorageLens	예	예	예	예	예	아니요	아니요	아니요
AWS::S3::StorageLensGroup	예	예	예	예	예	아니요	아니요	아니요
AWS::S3Express::BucketPolicy	예	아니요	아니요	아니요	예	아니요	아니요	아니요
AWS::S3Express::DirectoryBucket	예	아니요	아니요	아니요	예	아니요	아니요	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::SES::ConfigurationSet	예	예	예	예	예	예	아니요	아니요
AWS::SES::ContactList	예	예	예	예	예	예	아니요	아니요
AWS::SES::ReceiptFilter	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::SES::ReceiptRuleSet	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::SES::Template	예	예	예	예	예	예	아니요	아니요
AWS::SNS::Topic	예	예	예	예	예	예	예	예
AWS::SQS::Queue	예	예	예	예	예	예	아니요	아니요
AWS::SSM::AssociationCompliance	예	예	예	예	예	예	예	예
AWS::SSM::Document	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::SSM::FileData	예	예	예	예	예	예	예	예
AWS::SSM::ManagedInstanceInventory	예	예	예	예	예	예	예	예
AWS::SSM::PatchCompliance	예	예	예	예	예	예	예	예
AWS::SageMaker::AppImageConfig	예	예	예	예	예	예	예	아니요
AWS::SageMaker::CodeRepository	예	예	예	예	예	예	아니요	아니요
AWS::SageMaker::Domain	예	예	예	예	예	예	아니요	아니요
AWS::SageMaker::EndpointConfig	예	예	예	예	예	예	아니요	아니요
AWS::SageMaker::FeatureGroup	예	예	예	예	예	예	예	아니요
AWS::SageMaker::Image	예	예	예	예	예	예	예	아니요

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::SageMaker::InferenceExperiment	예	예	예	예	예	예	아니요	아니요
AWS::SageMaker::Model	예	예	예	예	예	예	아니요	아니요
AWS::SageMaker::NotebookInstance	예	예	예	예	예	예	아니요	아니요
AWS::SageMaker::NotebookInstanceLifecycleConfig	예	예	예	예	예	예	아니요	아니요
AWS::SageMaker::Workteam	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::SecretsManager::Secret	예	예	예	예	예	예	예	예
AWS::SecurityHub::Standard	예	예	예	예	예	예	예	예
AWS::ServiceCatalog::CloudFormationProduct	예	예	예	예	예	예	예	예
AWS::ServiceCatalog::CloudFormationProvisionedProduct	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::ServiceCatalog::Portfolio	예	예	예	예	예	예	예	예
AWS::ServiceDiscovery::HttpNamespace	예	예	예	예	예	예	예	예
AWS::ServiceDiscovery::Instance	예	예	예	예	예	예	아니요	아니요
AWS::ServiceDiscovery::PublicDnsNamespace	예	예	예	예	예	예	예	예
AWS::ServiceDiscovery::Service	예	예	예	예	예	예	아니요	아니요
AWS::ShieldRegional::Protection	예	예	예	예	예	예	아니요	아니요
AWS::Signer::SigningProfile	예	예	예	예	예	예	아니요	아니요
AWS::StepFunctions::Activity	예	예	예	예	예	예	예	예
AWS::StepFunctions::StateMachine	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::Transfer::Agreement	예	예	예	예	예	예	아니요	아니요
AWS::Transfer::Certificate	예	예	예	예	예	예	예	예
AWS::Transfer::Connector	예	예	예	예	예	예	예	예
AWS::Transfer::Profile	예	예	예	예	예	예	예	예
AWS::Transfer::Workflow	예	예	예	예	예	예	예	예
AWS::WAFRegional::RateBasedRule	예	예	예	예	예	예	예	예
AWS::WAFRegional::Rule	예	예	예	예	예	예	예	예
AWS::WAFRegional::RuleGroup	예	예	예	예	예	예	예	예
AWS::WAFRegional::WebACL	예	예	예	예	예	예	예	예
AWS::WAFv2::IPSet	예	예	예	예	예	예	예	예
AWS::WAFv2::ManagedRuleSet	예	예	예	예	예	예	예	예

리소스 유형	유럽(아일랜드)	유럽(프랑크푸르트)	유럽(런던)	유럽(파리)	유럽(스톡홀름)	유럽(밀라노)	유럽(스페인)	유럽(취리히)
AWS::WAFv2::RegexPatternSet	예	예	예	예	예	예	예	예
AWS::WAFv2::RuleGroup	예	예	예	예	예	예	예	예
AWS::WAFv2::WebACL	예	예	예	예	예	예	예	예
AWS::WorkSpaces::ConnectionAlias	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::WorkSpaces::Workspace	예	예	예	아니요	아니요	아니요	아니요	아니요
AWS::XRay::EncryptionConfig	예	예	예	예	예	예	예	예

아시아 태평양 리전

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::ACM::Certificate	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::ACMPCA::CertificateAuthority	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ACMPCA::CertificateAuthorityActivation	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::APS::RuleGroupsNamespace	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::AccessAnalyzer::Analyzer	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::AmazonMQ::Broker	예	아니요	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Amplify::App	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::Amplify::Branch	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::ApiGateway::RestApi	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::ApiGateway::Stage	예	예	예	예	예	예	예	예	예	예	아니요	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::ApiGatewayV2::Api	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::ApiGatewayV2::Stage	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::AppConfig::Application	예	아니요	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::AppConfig::ConfigurationProfile	예	아니요	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::AppConfig::DeploymentStrategy	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::AppConfig::Environment	예	아니요	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::AppConfig::ExtensionAssociation	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::AppConfig::HostedConfigurationVersion	예	아니요	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::AppFlow::Flow	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::AppIntegrations::Application	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::AppIntegrations::EventIntegration	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예
AWS::AppMesh::GatewayRoute	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::AppMesh::Mesh	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::AppMesh::Route	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::AppMesh::VirtualGateway	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::AppMesh::VirtualNode	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::AppMesh::VirtualRouter	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::AppMesh::VirtualService	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::AppRunner::Service	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	예	예	아니요	아니요	예
AWS::AppRunner::VpcConnector	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::AppStream::Application	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::AppStream::DirectoryConfig	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::AppStream::Fleet	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::AppStream::Stack	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::AppSync::ApiCache	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::AppSync::GraphQLApi	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Athena::DataCatalog	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Athena::PreparedStatement	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Athena::WorkGroup	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::AuditManager::Assessment	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Auto Scaling::AutoScalingGroup	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Auto Scaling:: LaunchConfiguration	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Auto Scaling:: ScalingPolicy	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Auto Scaling:: ScheduledAction	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Auto Scaling:: WarmPool	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Backup::BackupPlan	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Backup::BackupSelection	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Backup::BackupVault	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Backup::RecoveryPoint	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Backup::ReportPlan	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Batch::ComputeEnvironment	예	예	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::Batch::JobQueue	예	예	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::Batch::SchedulingPolicy	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Bedrock::Guardrail	아니요	예	아니요	아니요	아니요	예	예	예	예	예	예	아니요	예
AWS::Bedrock::KnowledgeBase	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	예	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Cassandra::Keyspace	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Cloud9::EnvironmentEC2	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::CloudFormation::Stack	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::CloudTrail::Trail	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::CloudWatch::Alarm	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::CloudWatch::MetricStream	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::CodeArtifact::Repository	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	예	예	아니요	아니요	예
AWS::CodeBuild::Project	예	예	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::CodeBuild::ReportGroup	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::CodeDeploy::Application	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::CodeDeploy::DeploymentConfig	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::CodeDeploy::DeploymentGroup	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::CodeGuruProfiler::ProfilingGroup	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	예
AWS::CodeGuruReviewer::RepositoryAssociation	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	예
AWS::CodePipeline::Pipeline	예	예	아니요	아니요	예	예	아니요	예	예	예	아니요	아니요	예
AWS::Cognito::IdentityPool	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Cognito::UserPool	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Cognito::UserPoolClient	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Cognito::UserPoolGroup	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Config::ConfigurationRecorder	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Config::ConformancePackCompliance	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Config::ResourceCompliance	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Connect::Instance	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예
AWS::Connect::PhoneNumber	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예
AWS::Connect::QuickConnect	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예
AWS::Connect::Rule	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Connect::User	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예
AWS::CustomerProfiles::Domain	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예
AWS::CustomerProfiles::ObjectType	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예
AWS::DMS::Certificate	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::DMS::Endpoint	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::DMS::EventSubscription	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::DMS::ReplicationInstance	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::DMS::ReplicationSubnetGroup	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::DMS::ReplicationTask	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::DataSync::LocationEFS	예	아니요	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::DataSync::LocationFSxLustre	예	아니요	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::DataSync::LocationFSxWindows	예	아니요	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::DataSync::LocationHDFS	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::DataSync::LocationNFS	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::DataSync::LocationObjectStorage	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::DataSync::LocationS3	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::DataSync::LocationSMB	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::DataSync::Task	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Detective::Graph	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::DynamoDB::Table	예	예	예	예	예	예	예	예	예	예	예	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EC2::Capacity Reservation	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::CarrierGateway	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	아니요	예	아니요	아니요	예
AWS::EC2::ClientVpnEndpoint	예	아니요	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::ClientVpnTargetNetworkAssociation	예	아니요	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::Customer Gateway	예	예	예	예	예	예	예	예	예	예	예	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EC2::DHCPOptions	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::EC2Fleet	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::EIP	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::EIPAssociation	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::EC2::EgressOnlyInternetGateway	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EC2::FlowLog	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::EC2::Host	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::IPAM	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::IPAMPool	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::IPAMResourceDiscovery	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EC2::IPAMResourceDiscoveryAssociation	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::IPAMScope	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::Instance	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::InstanceConnectEndpoint	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::InternetGateway	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::LaunchTemplate	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EC2::NatGateway	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::EC2::NetworkAcl	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::NetworkInsightsAccessScope	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::EC2::NetworkInsightsAccessScopeAnalysis	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::EC2::NetworkInsightsAnalysis	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EC2::NetworkInsightsPath	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::EC2::NetworkInterface	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::PrefixList	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::RegisteredHAInstance	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::EC2::RouteTable	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::SecurityGroup	예	예	예	예	예	예	예	예	예	예	예	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EC2::SnapshotBlockPublicAccess	예	예	예	예	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::SpotFleet	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::Subnet	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::SubnetRouteTableAssociation	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::TrafficMirrorFilter	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EC2::TrafficMirrorSession	예	아니요	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::TrafficMirrorTarget	예	아니요	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::TransitGateway	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::TransitGatewayAttachment	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::TransitGatewayConnect	예	아니요	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EC2::TransitGatewayMulticastDomain	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::TransitGatewayRouteTable	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::EC2::VPC	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::VPCBlockPublicAccessExclusion	예	예	예	예	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::VPCBlockPublicAccessOptions	예	예	예	예	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::VPCEndpoint	예	예	예	예	예	예	예	예	예	예	예	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EC2::VPCEndpointConnectionNotification	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::EC2::VPCEndpointService	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::VPCPeeringConnection	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::VPNConnection	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EC2::VPNConnectionRoute	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EC2::VPNGateway	예	예	예	예	예	예	예	예	예	예	예	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EC2::Volume	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::ECR::PullThroughCacheRule	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ECR::RegistryPolicy	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ECR::Repository	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ECS::CapacityProvider	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ECS::Cluster	예	예	예	예	예	예	예	예	예	예	예	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::ECS::Service	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::ECS::TaskDefinition	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::ECS::TaskSet	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EFS::AccessPoint	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EFS::FileSystem	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EKS::Addon	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::EKS::Cluster	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EKS::FargateProfile	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EKS::IdentityProviderConfig	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::EMR::SecurityConfiguration	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ElasticBeanstalk::Application	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::ElasticBeanstalk::ApplicationVersion	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::ElasticBeanstalk::Environment	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::ElasticLoadBalancing::LoadBalancer	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::ElasticLoadBalancingV2::Listener	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::ElasticLoadBalancingV2::LoadBalancer	예	예	예	예	예	예	예	예	예	예	예	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Elasticsearch::Domain	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::EventSchemas::Discoverer	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::EventSchemas::Registry	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::EventSchemas::RegistryPolicy	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::EventSchemas::Schema	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Events::ApiDestination	예	예	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::Events::Archive	예	예	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::Events::Connection	예	예	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::Events::Endpoint	아니요	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::Events::EventBus	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Events::Rule	예	예	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Evidently::Launch	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	예
AWS::Evidently::Project	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	예
AWS::Evidently::Segment	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	예
AWS::FIS::ExperimentTemplate	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Forecast::Dataset	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Forecast::DatasetGroup	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::FraudDetector::EntityType	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	아니요
AWS::FraudDetector::Label	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	아니요
AWS::FraudDetector::Outcome	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	아니요

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::FraudDetector::Variable	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	아니요
AWS::Glue::Classifier	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Glue::Job	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Glue::MLTransform	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Grafana::Workspace	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::GreengrassV2::ComponentVersion	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::GroundStation::Config	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	아니요
AWS::GroundStation::DataflowEndpointGroup	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	아니요
AWS::GroundStation::MissionProfile	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	아니요
AWS::GuardDuty::Detector	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::GuardDuty::Filter	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::GuardDuty::IPSet	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::GuardDuty::ThreatIntelSet	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::HealthLake::FHIRDatastore	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
AWS::IAM::Group	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::IAM::Policy	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::IAM::Role	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::IAM::User	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::IVS::Channel	아니요	아니요	아니요	아니요	아니요	예	아니요	예	아니요	아니요	아니요	아니요	예
AWS::IVS::PlaybackKeyPair	아니요	아니요	아니요	아니요	아니요	예	아니요	예	아니요	아니요	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::IVS::RecordingConfiguration	아니요	아니요	아니요	아니요	아니요	예	아니요	예	아니요	아니요	아니요	아니요	예
AWS::ImageBuilder::ContainerRecipe	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ImageBuilder::DistributionConfiguration	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ImageBuilder::ImagePipeline	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ImageBuilder::ImageRecipe	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::ImageBuilder::InfrastructureConfiguration	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::InspectorV2::Activation	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::InspectorV2::Filter	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::IoT::AccountAuditConfiguration	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoT::Authorizer	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::IoT::CACertificate	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoT::CustomMetric	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoT::Dimension	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoT::FleetMetric	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoT::JobTemplate	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::IoT::MitigationAction	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoT::Policy	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoT::ProvisioningTemplate	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoT::RoleAlias	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoT::ScheduledAudit	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::IoT::SecurityProfile	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTAnalytics::Channel	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	아니요	예	아니요	아니요	예
AWS::IoTAnalytics::Dataset	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	아니요	예	아니요	아니요	예
AWS::IoTAnalytics::Datastore	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	아니요	예	아니요	아니요	예
AWS::IoTAnalytics::Pipeline	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	아니요	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::IoTEvents::AlarmModel	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTEvents::DetectorModel	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTEvents::Input	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTSiteWise::AssetModel	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTSiteWise::Dashboard	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::IoTSiteWise::Gateway	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTSiteWise::Portal	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTSiteWise::Project	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTTwinMaker::ComponentType	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTTwinMaker::Entity	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	아니요

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::IoTTwinMaker::Scene	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTTwinMaker::SyncJob	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTTwinMaker::Workspace	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::IoTWireless::FuotaTask	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	예
AWS::IoTWireless::MulticastGroup	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::IoTWireless::ServiceProfile	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	예
AWS::KMS::Alias	예	예	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::KMS::Key	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::KafkaConnect::Connector	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Kendra::Index	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Kinesis::Stream	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Kinesis::StreamConsumer	예	예	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::KinesisAnalyticsV2::Application	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::KinesisFirehose::DeliveryStream	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::KinesisVideo::SignalingChannel	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::KinesisVideo::Stream	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Lambda::CodeSigningConfig	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Lambda::Function	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Lex::Bot	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예
AWS::Lex::BotAlias	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Lightsail::Bucket	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Lightsail::Certificate	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Lightsail::Disk	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Lightsail::StaticIp	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Logs::Destination	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::LookoutMetrics::Alert	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	예
AWS::LookoutVision::Project	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	아니요	아니요	예
AWS::M2::Environment	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::MSK::BatchScramSecret	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::MSK::Cluster	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::MSK::ClusterPolicy	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::MSK::Configuration	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::MSK::VpcConnection	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Macie::Session	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::MediaConnect::FlowEntitlement	예	예	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::MediaConnect::FlowSource	예	예	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::MediaConnect::FlowVpcInterface	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::MediaConnect::Gateway	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::MediaPackage::PackagingConfiguration	아니요	아니요	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::MediaPackage::PackagingGroup	아니요	아니요	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::MediaTailor::PlaybackConfiguration	아니요	아니요	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::MemoryDB::SubnetGroup	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::NetworkFirewall::Firewall	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::NetworkFirewall::FirewallPolicy	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::NetworkFirewall::RuleGroup	예	예	예	예	예	예	예	예	예	예	아니요	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::NetworkFirewall::TLSInspectionConfiguration	예	예	아니요	예	예	예	예	예	예	예	아니요	예	예
AWS::NetworkFirewall::VpcEndpointAssociation	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::OpenSearch::Domain	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::OpenSearchServerless::Collection	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	예	예	아니요	아니요	예
AWS::OpenSearchServerless::VpcEndpoint	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Panorama::Package	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	아니요
AWS::Personalize::Dataset	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Personalize::DatasetGroup	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Personalize::Schema	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Personalize::Solution	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Pinpoint::App	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Pinpoint::ApplicationSettings	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Pinpoint::Campaign	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Pinpoint::EmailChannel	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Pinpoint::EmailTemplate	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Pinpoint::EventStream	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Pinpoint::InAppTemplate	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Pinpoint::Segment	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::QLDB::Ledger	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예
AWS::QuickSight::DataSource	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::QuickSight::Template	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::QuickSight::Theme	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::RDS::DBCluster	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::RDS::DBClusterSnapshot	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::RDS::DBInstance	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::RDS::DBSecurityGroup	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::RDS::DBSnapshot	예	예	예	예	예	예	예	예	예	예	예	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::RDS::DBSubnetGroup	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::RDS::EventSubscription	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::RDS::GlobalCluster	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::RDS::OptionGroup	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::RUM::AppMonitor	아니요	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Redshift::Cluster	예	예	예	예	예	예	예	예	예	예	예	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Redshift::ClusterParameterGroup	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Redshift::ClusterSecurityGroup	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Redshift::ClusterSnapshot	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Redshift::ClusterSubnetGroup	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Redshift::EndpointAccess	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::Redshift::EndpointAuthorization	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Redshift::EventSubscription	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::Redshift::ScheduledAction	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::ResilienceHub::App	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::ResilienceHub::ResiliencyPolicy	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::ResourceExplorer2::Index	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::RoboMaker::RobotApplication	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	아니요	예
AWS::RoboMaker::RobotApplicationVersion	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	아니요	예
AWS::RoboMaker::SimulationApplication	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	아니요	예
AWS::Route53Profiles::Profile	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Route53Resolver::FirewallDomainList	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Route53Resolver::FirewallRuleGroup	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::Route53Resolver::FirewallRuleGroupAssociation	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::Route53Resolver::ResolverEndpoint	예	예	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Route53Resolver::ResolverQueryLoggingConfig	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::Route53Resolver::ResolverRule	예	예	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Route53Resolver::ResolverRuleAssociation	예	예	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::S3::AccessPoint	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::S3::AccountPublicAccessBlock	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::S3::Bucket	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::S3::StorageLens	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::S3::StorageLensGroup	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::S3Express::BucketPolicy	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::S3Express::DirectoryBucket	아니요	아니요	아니요	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요	아니요	예
AWS::SES::ConfigurationSet	아니요	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SES::ContactList	아니요	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SES::ReceiptFilter	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	예
AWS::SES::ReceiptRuleSet	아니요	아니요	예	아니요	아니요	아니요	아니요	아니요	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::SES::Template	아니요	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SNS::Topic	예	예	예	예	예	예	예	예	예	예	예	예	예
AWS::SQS::Queue	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SSM::AssociationCompliance	예	예	예	예	예	예	아니요	예	예	예	아니요	예	예
AWS::SSM::Document	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::SSM::FileData	예	예	예	예	예	예	아니요	예	예	예	아니요	예	예
AWS::SSM::ManagedInstanceInventory	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::SSM::PatchCompliance	예	예	예	예	예	예	아니요	예	예	예	아니요	예	예
AWS::SageMaker::AppImageConfig	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SageMaker::CodeRepository	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::SageMaker::Domain	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SageMaker::EndpointConfig	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SageMaker::FeatureGroup	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SageMaker::Image	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SageMaker::InferenceExperiment	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::SageMaker::Model	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SageMaker::NotebookInstance	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SageMaker::NotebookInstanceLifecycleConfig	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::SageMaker::Workteam	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::SecretsManager::Secret	예	예	예	예	예	예	예	예	예	예	예	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::SecurityHub::Standard	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::ServiceCatalog::CloudFormationProduct	예	예	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ServiceCatalog::CloudFormationProvisionedProduct	예	예	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ServiceCatalog::Portfolio	예	예	아니요	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::ServiceDiscovery::HttpNamespace	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ServiceDiscovery::Instance	예	아니요	아니요	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::ServiceDiscovery::PublicDnsNamespace	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::ServiceDiscovery::Service	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::ShieldRegional::Protection	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Signer::SigningProfile	예	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::StepFunctions::Activity	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::StepFunctions::StateMachine	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Transfer::Agreement	예	아니요	예	아니요	아니요	예	예	예	예	예	아니요	아니요	예
AWS::Transfer::Certificate	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::Transfer::Connector	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Transfer::Profile	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::Transfer::Workflow	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::WAFRegional::RateBasedRule	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::WAFRegional::Rule	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::WAFRegional::RuleGroup	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::WAFRegional::WebACL	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예
AWS::WAFv2::IPSet	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::WAFv2::ManagedRuleSet	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::WAFv2::RegexPatternSet	예	예	예	예	예	예	예	예	예	예	아니요	예	예

리소스 유형	아시아 태평양 (홍콩)	아시아 태평양 (하이데라바드)	아시아 태평양 (자카르타)	아시아 태평양 (말레이시아)	아시아 태평양 (멜버른)	아시아 태평양 (뭄바이)	아시아 태평양 (오사카)	아시아 태평양 (서울)	아시아 태평양 (싱가포르)	아시아 태평양 (시드니)	아시아 태평양 (타이베이)	아시아 태평양 (태국)	아시아 태평양 (도쿄)
AWS::WAFv2::RuleGroup	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::WAFv2::WebACL	예	예	예	예	예	예	예	예	예	예	아니요	예	예
AWS::WorkSpaces::ConnectionAlias	아니요	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요	예
AWS::WorkSpaces::Workspace	아니요	아니요	아니요	아니요	아니요	예	아니요	예	예	예	아니요	아니요	예
AWS::XRay::EncryptionConfig	예	예	예	아니요	예	예	예	예	예	예	아니요	아니요	예

중국 리전

리소스 유형	중국(베이징)	중국(닝샤)
AWS::ACM::Certificate	예	예
AWS::AmazonMQ::Broker	예	예
AWS::ApiGateway::RestApi	예	예
AWS::ApiGateway::Stage	예	예
AWS::ApiGatewayV2::Api	예	예
AWS::ApiGatewayV2::Stage	예	예
AWS::AppConfig::Application	예	예
AWS::AppConfig::ConfigurationProfile	예	예
AWS::AppConfig::DeploymentStrategy	예	예
AWS::AppConfig::Environment	예	예
AWS::AppConfig::ExtensionAssociation	예	예
AWS::AppConfig::HostedConfigurationVersion	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::AppSync::ApiCache	예	예
AWS::AppSync::GraphQLApi	예	예
AWS::Athena::DataCatalog	예	예
AWS::Athena::PreparedStatement	예	예
AWS::Athena::WorkGroup	예	예
AWS::AutoScaling::AutoScalingGroup	예	예
AWS::AutoScaling::LaunchConfiguration	예	예
AWS::AutoScaling::ScalingPolicy	예	예
AWS::AutoScaling::ScheduledAction	예	예
AWS::AutoScaling::WarmPool	예	예
AWS::Backup::BackupPlan	예	예
AWS::Backup::BackupSelection	예	예
AWS::Backup::BackupVault	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::Backup::RecoveryPoint	예	예
AWS::Batch::ComputeEnvironment	예	예
AWS::Batch::JobQueue	예	예
AWS::Batch::SchedulingPolicy	예	예
AWS::Cassandra::Keyspace	예	예
AWS::CloudFormation::Stack	예	예
AWS::CloudTrail::Trail	예	예
AWS::CloudWatch::Alarm	예	예
AWS::CloudWatch::MetricStream	예	예
AWS::CodeBuild::Project	예	예
AWS::CodeBuild::ReportGroup	예	예
AWS::Cognito::IdentityPool	예	아니요
AWS::Config::ConfigurationRecorder	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::Config::ResourceCompliance	예	예
AWS::DMS::Certificate	예	예
AWS::DMS::Endpoint	예	예
AWS::DMS::EventSubscription	예	예
AWS::DMS::ReplicationInstance	예	예
AWS::DMS::ReplicationSubnetGroup	예	예
AWS::DMS::ReplicationTask	예	예
AWS::DataSync::LocationEFS	예	예
AWS::DataSync::LocationHDFS	예	예
AWS::DataSync::LocationNFS	예	예
AWS::DataSync::LocationObjectStorage	예	예
AWS::DataSync::LocationS3	예	예
AWS::DataSync::LocationSMB	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::DataSync::Task	예	예
AWS::DynamoDB::Table	예	예
AWS::EC2::CapacityReservation	예	예
AWS::EC2::DHCPOptions	예	예
AWS::EC2::EC2Fleet	예	예
AWS::EC2::EIP	예	예
AWS::EC2::EIPAssociation	예	예
AWS::EC2::FlowLog	예	예
AWS::EC2::Host	예	예
AWS::EC2::Instance	예	예
AWS::EC2::InternetGateway	예	예
AWS::EC2::LaunchTemplate	예	예
AWS::EC2::NatGateway	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::EC2::NetworkAcl	예	예
AWS::EC2::NetworkInterface	예	예
AWS::EC2::PrefixList	예	예
AWS::EC2::RouteTable	예	예
AWS::EC2::SecurityGroup	예	예
AWS::EC2::SnapshotBlockPublicAccess	예	예
AWS::EC2::SpotFleet	예	예
AWS::EC2::Subnet	예	예
AWS::EC2::SubnetRouteTableAssociation	예	예
AWS::EC2::TrafficMirrorFilter	예	예
AWS::EC2::TrafficMirrorSession	예	예
AWS::EC2::TrafficMirrorTarget	예	예
AWS::EC2::TransitGateway	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::EC2::TransitGatewayAttachment	예	예
AWS::EC2::TransitGatewayConnect	예	예
AWS::EC2::TransitGatewayMulticastDomain	예	예
AWS::EC2::TransitGatewayRouteTable	예	예
AWS::EC2::VPC	예	예
AWS::EC2::VPCBlockPublicAccessExclusion	예	예
AWS::EC2::VPCBlockPublicAccessOptions	예	예
AWS::EC2::VPCEndpoint	예	예
AWS::EC2::VPCEndpointConnectionNotification	예	예
AWS::EC2::VPCEndpointService	예	예
AWS::EC2::VPCPeeringConnection	예	예
AWS::EC2::VPNGateway	예	아니요
AWS::EC2::Volume	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::ECR::Repository	예	예
AWS::ECS::CapacityProvider	예	예
AWS::ECS::Cluster	예	예
AWS::ECS::Service	예	예
AWS::ECS::TaskDefinition	예	예
AWS::ECS::TaskSet	예	예
AWS::EFS::AccessPoint	예	예
AWS::EFS::FileSystem	예	예
AWS::EKS::Addon	예	예
AWS::EKS::Cluster	예	예
AWS::EKS::FargateProfile	예	예
AWS::EKS::IdentityProviderConfig	예	예
AWS::EMR::SecurityConfiguration	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::ElasticBeanstalk::Application	예	예
AWS::ElasticBeanstalk::ApplicationVersion	예	예
AWS::ElasticBeanstalk::Environment	예	예
AWS::ElasticLoadBalancing::LoadBalancer	예	예
AWS::ElasticLoadBalancingV2::Listener	예	예
AWS::ElasticLoadBalancingV2::LoadBalancer	예	예
AWS::Elasticsearch::Domain	예	예
AWS::Events::Archive	예	예
AWS::Events::EventBus	예	예
AWS::Events::Rule	예	예
AWS::Glue::Classifier	예	예
AWS::Glue::Job	예	예
AWS::Glue::MLTransform	예	아니요

리소스 유형	중국(베이징)	중국(닝샤)
AWS::GreengrassV2::ComponentVersion	예	아니요
AWS::GuardDuty::Filter	예	예
AWS::GuardDuty::ThreatIntelSet	예	예
AWS::IAM::Group	예	예
AWS::IAM::InstanceProfile	예	아니요
AWS::IAM::OIDCProvider	예	아니요
AWS::IAM::Policy	예	예
AWS::IAM::Role	예	예
AWS::IAM::SAMLProvider	예	아니요
AWS::IAM::ServerCertificate	예	아니요
AWS::IAM::User	예	예
AWS::ImageBuilder::ContainerRecipe	예	예
AWS::ImageBuilder::DistributionConfiguration	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::ImageBuilder::ImagePipeline	예	예
AWS::ImageBuilder::ImageRecipe	예	예
AWS::ImageBuilder::InfrastructureConfiguration	예	예
AWS::InspectorV2::Activation	예	예
AWS::IoT::AccountAuditConfiguration	예	예
AWS::IoT::Authorizer	예	예
AWS::IoT::CACertificate	예	예
AWS::IoT::CustomMetric	예	예
AWS::IoT::Dimension	예	예
AWS::IoT::FleetMetric	예	예
AWS::IoT::JobTemplate	예	예
AWS::IoT::MitigationAction	예	예
AWS::IoT::Policy	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::IoT::ProvisioningTemplate	예	예
AWS::IoT::RoleAlias	예	예
AWS::IoT::ScheduledAudit	예	예
AWS::IoT::SecurityProfile	예	예
AWS::IoTAnalytics::Channel	예	아니요
AWS::IoTAnalytics::Dataset	예	아니요
AWS::IoTAnalytics::Datastore	예	아니요
AWS::IoTAnalytics::Pipeline	예	아니요
AWS::IoTEvents::AlarmModel	예	아니요
AWS::IoTEvents::DetectorModel	예	아니요
AWS::IoTEvents::Input	예	아니요
AWS::IoTSiteWise::AssetModel	예	아니요
AWS::IoTSiteWise::Dashboard	예	아니요

리소스 유형	중국(베이징)	중국(닝샤)
AWS::IoTSiteWise::Gateway	예	아니요
AWS::IoTSiteWise::Portal	예	아니요
AWS::IoTSiteWise::Project	예	아니요
AWS::KMS::Alias	예	예
AWS::KMS::Key	예	예
AWS::Kinesis::Stream	예	예
AWS::Kinesis::StreamConsumer	예	예
AWS::KinesisAnalyticsV2::Application	예	예
AWS::KinesisFirehose::DeliveryStream	예	예
AWS::Lambda::Function	예	아니요
AWS::Logs::Destination	예	예
AWS::MSK::BatchScramSecret	예	예
AWS::MSK::Cluster	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::MSK::ClusterPolicy	예	예
AWS::MSK::Configuration	예	예
AWS::MSK::VpcConnection	예	예
AWS::NetworkFirewall::Firewall	예	예
AWS::NetworkFirewall::FirewallPolicy	예	예
AWS::NetworkFirewall::RuleGroup	예	예
AWS::NetworkFirewall::TLSInspectionConfiguration	예	예
AWS::NetworkFirewall::VpcEndpointAssociation	예	예
AWS::OpenSearch::Domain	예	예
AWS::Personalize::Dataset	예	아니요
AWS::Personalize::DatasetGroup	예	아니요
AWS::Personalize::Schema	예	아니요
AWS::Personalize::Solution	예	아니요

리소스 유형	중국(베이징)	중국(닝샤)
AWS::RDS::DBCluster	아니요	예
AWS::RDS::DBClusterSnapshot	예	예
AWS::RDS::DBInstance	예	예
AWS::RDS::DBSecurityGroup	예	예
AWS::RDS::DBSnapshot	예	예
AWS::RDS::DBSubnetGroup	예	예
AWS::RDS::EventSubscription	예	예
AWS::RDS::OptionGroup	예	예
AWS::Redshift::Cluster	예	예
AWS::Redshift::ClusterParameterGroup	예	예
AWS::Redshift::ClusterSecurityGroup	예	예
AWS::Redshift::ClusterSnapshot	예	예
AWS::Redshift::ClusterSubnetGroup	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::Redshift::EventSubscription	예	예
AWS::Route53Profiles::Profile	예	예
AWS::Route53Resolver::FirewallDomainList	예	예
AWS::Route53Resolver::FirewallRuleGroupAssociation	예	예
AWS::Route53Resolver::ResolverEndpoint	예	예
AWS::Route53Resolver::ResolverQueryLoggingConfig	예	예
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	예	예
AWS::Route53Resolver::ResolverRule	예	예
AWS::Route53Resolver::ResolverRuleAssociation	예	예
AWS::S3::AccessPoint	예	예
AWS::S3::AccountPublicAccessBlock	예	예
AWS::S3::Bucket	예	예
AWS::S3::StorageLensGroup	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::SES::ConfigurationSet	아니요	예
AWS::SES::ContactList	아니요	예
AWS::SES::Template	아니요	예
AWS::SNS::Topic	예	예
AWS::SQS::Queue	예	예
AWS::SSM::AssociationCompliance	예	예
AWS::SSM::Document	예	예
AWS::SSM::FileData	예	예
AWS::SSM::ManagedInstanceInventory	예	예
AWS::SSM::PatchCompliance	예	예
AWS::SageMaker::AppImageConfig	예	예
AWS::SageMaker::CodeRepository	예	예
AWS::SageMaker::Domain	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::SageMaker::EndpointConfig	예	예
AWS::SageMaker::FeatureGroup	예	예
AWS::SageMaker::Image	예	예
AWS::SageMaker::Model	예	예
AWS::SageMaker::NotebookInstance	예	예
AWS::SageMaker::NotebookInstanceLifecycleConfig	예	예
AWS::SecretsManager::Secret	예	예
AWS::SecurityHub::Standard	예	예
AWS::ServiceCatalog::CloudFormationProduct	예	예
AWS::ServiceCatalog::CloudFormationProvisionedProduct	예	예
AWS::ServiceCatalog::Portfolio	예	예
AWS::ServiceDiscovery::HttpNamespace	예	예
AWS::ServiceDiscovery::Instance	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::ServiceDiscovery::PublicDnsNamespace	예	예
AWS::ServiceDiscovery::Service	예	예
AWS::StepFunctions::Activity	예	아니요
AWS::StepFunctions::StateMachine	예	예
AWS::Transfer::Agreement	예	예
AWS::Transfer::Certificate	예	예
AWS::Transfer::Connector	예	예
AWS::Transfer::Profile	예	예
AWS::Transfer::Workflow	예	예
AWS::WAFRegional::RateBasedRule	예	예
AWS::WAFRegional::Rule	예	예
AWS::WAFRegional::RuleGroup	예	예
AWS::WAFRegional::WebACL	예	예

리소스 유형	중국(베이징)	중국(닝샤)
AWS::WAFv2::IPSet	예	예
AWS::WAFv2::ManagedRuleSet	예	예
AWS::WAFv2::RegexPatternSet	예	예
AWS::WAFv2::RuleGroup	예	예
AWS::WAFv2::WebACL	예	예
AWS::WorkSpaces::Workspace	아니요	예

아프리카 및 중동 리전

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::ACM::Certificate	예	예	예	예
AWS::ACMPCA::CertificateAuthority	예	예	예	예
AWS::ACMPCA::CertificateAuthorityActivation	예	예	예	예
AWS::AccessAnalyzer::Analyzer	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::AmazonMQ::Broker	예	아니요	예	예
AWS::Amplify::App	아니요	아니요	예	아니요
AWS::Amplify::Branch	아니요	아니요	예	아니요
AWS::ApiGateway::RestApi	예	예	예	예
AWS::ApiGateway::Stage	예	예	예	예
AWS::ApiGatewayV2::Api	예	예	예	예
AWS::ApiGatewayV2::Stage	예	예	예	예
AWS::AppConfig::Application	예	예	예	아니요
AWS::AppConfig::ConfigurationProfile	예	예	예	아니요
AWS::AppConfig::DeploymentStrategy	예	예	예	예
AWS::AppConfig::Environment	예	예	예	아니요
AWS::AppConfig::ExtensionAssociation	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::AppConfig::HostedConfigurationVersion	예	예	예	아니요
AWS::AppFlow::Flow	예	아니요	아니요	아니요
AWS::AppIntegrations::Application	예	아니요	아니요	아니요
AWS::AppIntegrations::EventIntegration	예	아니요	아니요	아니요
AWS::AppMesh::GatewayRoute	예	예	예	아니요
AWS::AppMesh::Mesh	예	예	예	아니요
AWS::AppMesh::Route	예	예	예	아니요
AWS::AppMesh::VirtualGateway	예	예	예	아니요
AWS::AppMesh::VirtualNode	예	예	예	아니요
AWS::AppMesh::VirtualRouter	예	예	예	아니요
AWS::AppMesh::VirtualService	예	예	예	아니요
AWS::AppSync::ApiCache	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::AppSync::GraphQLApi	예	예	예	예
AWS::Athena::DataCatalog	예	예	예	예
AWS::Athena::PreparedStatement	예	예	예	예
AWS::Athena::WorkGroup	예	예	예	예
AWS::AutoScaling::AutoScalingGroup	예	예	예	예
AWS::AutoScaling::LaunchConfiguration	예	예	예	예
AWS::AutoScaling::ScalingPolicy	예	예	예	예
AWS::AutoScaling::ScheduledAction	예	예	예	예
AWS::AutoScaling::WarmPool	예	아니요	예	아니요
AWS::Backup::BackupPlan	예	예	예	예
AWS::Backup::BackupSelection	예	예	예	예
AWS::Backup::BackupVault	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::Backup::RecoveryPoint	예	예	예	예
AWS::Backup::ReportPlan	예	아니요	예	아니요
AWS::Batch::ComputeEnvironment	예	아니요	예	예
AWS::Batch::JobQueue	예	아니요	예	예
AWS::Batch::SchedulingPolicy	예	예	예	예
AWS::Cassandra::Keyspace	아니요	아니요	예	아니요
AWS::Cloud9::EnvironmentEC2	예	아니요	예	아니요
AWS::CloudFormation::Stack	예	아니요	예	아니요
AWS::CloudTrail::Trail	예	예	예	예
AWS::CloudWatch::Alarm	예	예	예	예
AWS::CloudWatch::MetricStream	예	예	예	예
AWS::CodeBuild::Project	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::CodeBuild::ReportGroup	예	예	예	예
AWS::CodeDeploy::Application	예	아니요	예	아니요
AWS::CodeDeploy::DeploymentConfig	예	아니요	예	아니요
AWS::CodeDeploy::DeploymentGroup	예	아니요	예	아니요
AWS::CodePipeline::Pipeline	아니요	예	아니요	예
AWS::Cognito::IdentityPool	예	예	예	예
AWS::Cognito::UserPool	예	예	예	예
AWS::Cognito::UserPoolClient	예	예	예	예
AWS::Cognito::UserPoolGroup	예	예	예	예
AWS::Config::ConfigurationRecorder	예	예	예	예
AWS::Config::ConformancePackCompliance	예	예	예	예
AWS::Config::ResourceCompliance	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::Connect::Instance	예	아니요	아니요	아니요
AWS::Connect::PhoneNumber	예	아니요	아니요	아니요
AWS::Connect::QuickConnect	예	아니요	아니요	아니요
AWS::Connect::Rule	예	아니요	아니요	아니요
AWS::Connect::User	예	아니요	아니요	아니요
AWS::CustomerProfiles::Domain	예	아니요	아니요	아니요
AWS::CustomerProfiles::ObjectType	예	아니요	아니요	아니요
AWS::DMS::Certificate	예	아니요	예	아니요
AWS::DMS::Endpoint	예	아니요	예	아니요
AWS::DMS::EventSubscription	예	아니요	예	아니요
AWS::DMS::ReplicationInstance	예	아니요	예	아니요
AWS::DMS::ReplicationSubnetGroup	예	아니요	예	아니요

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::DMS::ReplicationTask	예	아니요	예	아니요
AWS::DataSync::LocationEFS	예	아니요	예	예
AWS::DataSync::LocationFSxLustre	예	아니요	예	아니요
AWS::DataSync::LocationFSxWindows	예	아니요	예	아니요
AWS::DataSync::LocationHDFS	예	아니요	예	예
AWS::DataSync::LocationNFS	예	아니요	예	예
AWS::DataSync::LocationObjectStorage	예	아니요	예	예
AWS::DataSync::LocationS3	예	예	예	예
AWS::DataSync::LocationSMB	예	아니요	예	예
AWS::DataSync::Task	예	예	예	예
AWS::Detective::Graph	예	예	예	아니요
AWS::DynamoDB::Table	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::EC2::CapacityReservation	예	예	예	예
AWS::EC2::ClientVpnEndpoint	예	아니요	예	아니요
AWS::EC2::ClientVpnTargetNetworkAssociation	예	예	예	아니요
AWS::EC2::CustomerGateway	예	예	예	예
AWS::EC2::DHCPOptions	예	예	예	예
AWS::EC2::EC2Fleet	예	아니요	예	예
AWS::EC2::EIP	예	예	예	예
AWS::EC2::EIPAssociation	예	예	예	예
AWS::EC2::EgressOnlyInternetGateway	예	아니요	예	예
AWS::EC2::FlowLog	예	아니요	예	예
AWS::EC2::Host	예	예	예	예
AWS::EC2::IPAM	예	아니요	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::EC2::IPAMPool	예	아니요	예	예
AWS::EC2::IPAMResourceDiscovery	예	예	예	예
AWS::EC2::IPAMResourceDiscoveryAssociation	예	예	예	예
AWS::EC2::IPAMScope	예	아니요	예	예
AWS::EC2::Instance	예	예	예	예
AWS::EC2::InstanceConnectEndpoint	예	예	예	예
AWS::EC2::InternetGateway	예	예	예	예
AWS::EC2::LaunchTemplate	예	아니요	예	아니요
AWS::EC2::NatGateway	예	아니요	예	예
AWS::EC2::NetworkAcl	예	예	예	예
AWS::EC2::NetworkInsightsAccessScope	예	아니요	예	아니요
AWS::EC2::NetworkInsightsAccessScopeAnalysis	예	아니요	예	아니요

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::EC2::NetworkInsightsAnalysis	예	아니요	예	아니요
AWS::EC2::NetworkInsightsPath	예	아니요	예	아니요
AWS::EC2::NetworkInterface	예	예	예	예
AWS::EC2::PrefixList	예	예	예	예
AWS::EC2::RouteTable	예	예	예	예
AWS::EC2::SecurityGroup	예	예	예	예
AWS::EC2::SnapshotBlockPublicAccess	예	예	예	예
AWS::EC2::SpotFleet	예	예	예	예
AWS::EC2::Subnet	예	예	예	예
AWS::EC2::SubnetRouteTableAssociation	예	예	예	예
AWS::EC2::TrafficMirrorFilter	예	예	예	예
AWS::EC2::TrafficMirrorSession	아니요	아니요	예	아니요

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::EC2::TrafficMirrorTarget	아니요	아니요	예	아니요
AWS::EC2::TransitGateway	예	예	예	예
AWS::EC2::TransitGatewayAttachment	예	아니요	예	예
AWS::EC2::TransitGatewayConnect	예	아니요	예	예
AWS::EC2::TransitGatewayMulticastDomain	예	예	예	예
AWS::EC2::TransitGatewayRouteTable	예	아니요	예	예
AWS::EC2::VPC	예	예	예	예
AWS::EC2::VPCBlockPublicAccessExclusion	예	예	예	예
AWS::EC2::VPCBlockPublicAccessOptions	예	예	예	예
AWS::EC2::VPCEndpoint	예	예	예	예
AWS::EC2::VPCEndpointConnectionNotification	예	예	예	예
AWS::EC2::VPCEndpointService	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::EC2::VPCPeeringConnection	예	예	예	예
AWS::EC2::VPNConnection	예	예	예	예
AWS::EC2::VPNConnectionRoute	예	예	예	예
AWS::EC2::VPNGateway	예	예	예	예
AWS::EC2::Volume	예	예	예	예
AWS::ECR::PullThroughCacheRule	예	예	예	예
AWS::ECR::RegistryPolicy	예	예	예	예
AWS::ECR::Repository	예	예	예	예
AWS::ECS::CapacityProvider	예	예	예	예
AWS::ECS::Cluster	예	예	예	예
AWS::ECS::Service	예	예	예	예
AWS::ECS::TaskDefinition	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::ECS::TaskSet	예	아니요	예	예
AWS::EFS::AccessPoint	예	예	예	예
AWS::EFS::FileSystem	예	예	예	예
AWS::EKS::Addon	예	아니요	예	예
AWS::EKS::Cluster	예	아니요	예	예
AWS::EKS::FargateProfile	예	예	예	예
AWS::EKS::IdentityProviderConfig	예	아니요	예	예
AWS::EMR::SecurityConfiguration	예	예	예	예
AWS::ElasticBeanstalk::Application	예	아니요	예	예
AWS::ElasticBeanstalk::ApplicationVersion	예	아니요	예	예
AWS::ElasticBeanstalk::Environment	예	아니요	예	예
AWS::ElasticLoadBalancing::LoadBalancer	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::ElasticLoadBalancingV2::Listener	예	아니요	예	아니요
AWS::ElasticLoadBalancingV2::LoadBalancer	예	예	예	예
AWS::Elasticsearch::Domain	예	예	예	예
AWS::EventSchemas::Discoverer	예	아니요	예	예
AWS::EventSchemas::Registry	예	아니요	예	예
AWS::EventSchemas::RegistryPolicy	예	아니요	예	예
AWS::EventSchemas::Schema	예	아니요	예	예
AWS::Events::ApiDestination	예	아니요	예	예
AWS::Events::Archive	예	아니요	예	예
AWS::Events::Connection	예	아니요	예	예
AWS::Events::EventBus	예	예	예	예
AWS::Events::Rule	예	아니요	예	아니요

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::FIS::ExperimentTemplate	예	아니요	예	아니요
AWS::Glue::Classifier	예	예	예	예
AWS::Glue::Job	예	예	예	예
AWS::Glue::MLTransform	예	예	예	예
AWS::GroundStation::Config	예	아니요	예	아니요
AWS::GroundStation ::DataflowEndpointGroup	예	아니요	예	아니요
AWS::GroundStation::MissionProfile	예	아니요	예	아니요
AWS::GuardDuty::Detector	예	예	예	예
AWS::GuardDuty::Filter	예	아니요	예	아니요
AWS::GuardDuty::IPSet	예	아니요	예	예
AWS::GuardDuty::ThreatIntelSet	예	예	예	예
AWS::IAM::Group	예	아니요	예	아니요

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::IAM::Policy	예	아니요	예	아니요
AWS::IAM::Role	예	아니요	예	아니요
AWS::IAM::User	예	아니요	예	아니요
AWS::ImageBuilder::ContainerRecipe	예	예	예	예
AWS::ImageBuilder::DistributionConfiguration	예	예	예	예
AWS::ImageBuilder::ImagePipeline	예	예	예	예
AWS::ImageBuilder::ImageRecipe	예	예	예	예
AWS::ImageBuilder::InfrastructureConfiguration	예	예	예	예
AWS::InspectorV2::Activation	예	아니요	예	아니요
AWS::InspectorV2::Filter	예	아니요	예	아니요
AWS::IoT::AccountAuditConfiguration	아니요	아니요	예	예
AWS::IoT::Authorizer	아니요	아니요	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::IoT::CACertificate	아니요	아니요	예	예
AWS::IoT::CustomMetric	아니요	아니요	예	예
AWS::IoT::Dimension	아니요	아니요	예	예
AWS::IoT::FleetMetric	아니요	아니요	예	예
AWS::IoT::JobTemplate	아니요	아니요	예	예
AWS::IoT::MitigationAction	아니요	아니요	예	예
AWS::IoT::Policy	아니요	아니요	예	예
AWS::IoT::ProvisioningTemplate	아니요	아니요	예	예
AWS::IoT::RoleAlias	아니요	아니요	예	예
AWS::IoT::ScheduledAudit	아니요	아니요	예	예
AWS::IoT::SecurityProfile	아니요	아니요	예	예
AWS::KMS::Alias	예	아니요	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::KMS::Key	예	예	예	예
AWS::Kinesis::Stream	예	아니요	예	예
AWS::Kinesis::StreamConsumer	예	예	예	예
AWS::KinesisAnalyticsV2::Application	예	예	예	예
AWS::KinesisFirehose::DeliveryStream	예	예	예	예
AWS::Lambda::CodeSigningConfig	예	아니요	예	아니요
AWS::Lambda::Function	예	예	예	예
AWS::Lex::Bot	예	아니요	아니요	아니요
AWS::Lex::BotAlias	예	아니요	아니요	아니요
AWS::Logs::Destination	예	예	예	예
AWS::MSK::BatchScramSecret	예	아니요	예	예
AWS::MSK::Cluster	예	아니요	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::MSK::ClusterPolicy	예	예	예	예
AWS::MSK::Configuration	예	예	예	예
AWS::MSK::VpcConnection	예	예	예	예
AWS::Macie::Session	예	예	예	아니요
AWS::MediaConnect::FlowEntitlement	예	아니요	아니요	예
AWS::MediaConnect::FlowSource	예	아니요	아니요	예
AWS::MediaConnect::FlowVpcInterface	예	아니요	아니요	아니요
AWS::MediaConnect::Gateway	예	아니요	아니요	아니요
AWS::MediaTailor::PlaybackConfiguration	예	아니요	아니요	예
AWS::NetworkFirewall::Firewall	예	예	예	예
AWS::NetworkFirewall::FirewallPolicy	예	예	예	예
AWS::NetworkFirewall::RuleGroup	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::NetworkFirewall::TLSInspectionConfiguration	예	예	예	예
AWS::NetworkFirewall::VpcEndpointAssociation	예	예	예	예
AWS::OpenSearch::Domain	예	아니요	예	아니요
AWS::RDS::DBCluster	예	예	예	예
AWS::RDS::DBClusterSnapshot	예	아니요	예	예
AWS::RDS::DBInstance	예	예	예	예
AWS::RDS::DBSecurityGroup	예	예	예	예
AWS::RDS::DBSnapshot	예	예	예	예
AWS::RDS::DBSubnetGroup	예	예	예	예
AWS::RDS::EventSubscription	예	예	예	예
AWS::RDS::GlobalCluster	예	예	예	예
AWS::RDS::OptionGroup	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::RUM::AppMonitor	아니요	아니요	예	예
AWS::Redshift::Cluster	예	예	예	예
AWS::Redshift::ClusterParameterGroup	예	예	예	예
AWS::Redshift::ClusterSecurityGroup	예	예	예	예
AWS::Redshift::ClusterSnapshot	예	예	예	예
AWS::Redshift::ClusterSubnetGroup	예	예	예	예
AWS::Redshift::EventSubscription	예	예	예	예
AWS::Redshift::ScheduledAction	아니요	아니요	예	아니요
AWS::ResilienceHub::App	예	아니요	예	아니요
AWS::ResilienceHub::ResiliencyPolicy	예	아니요	예	아니요
AWS::ResourceExplorer2::Index	아니요	아니요	예	예
AWS::Route53Profiles::Profile	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::Route53Resolver::FirewallDomainList	예	아니요	예	아니요
AWS::Route53Resolver::FirewallRuleGroup	예	아니요	예	아니요
AWS::Route53Resolver::FirewallRuleGroupAssociation	예	아니요	예	아니요
AWS::Route53Resolver::ResolverEndpoint	예	아니요	예	예
AWS::Route53Resolver::ResolverQueryLoggingConfig	예	아니요	예	아니요
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	예	아니요	예	아니요
AWS::Route53Resolver::ResolverRule	예	아니요	예	예
AWS::Route53Resolver::ResolverRuleAssociation	예	아니요	예	예
AWS::S3::AccessPoint	예	예	예	예
AWS::S3::AccountPublicAccessBlock	예	아니요	예	예
AWS::S3::Bucket	예	예	예	예
AWS::SES::ConfigurationSet	예	예	예	아니요

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::SES::ContactList	예	예	예	아니요
AWS::SES::Template	예	예	예	아니요
AWS::SNS::Topic	예	예	예	예
AWS::SQS::Queue	예	아니요	예	아니요
AWS::SSM::AssociationCompliance	예	예	예	예
AWS::SSM::Document	예	예	예	예
AWS::SSM::FileData	예	예	예	예
AWS::SSM::ManagedInstanceInventory	예	예	예	예
AWS::SSM::PatchCompliance	예	예	예	예
AWS::SageMaker::AppImageConfig	예	예	예	예
AWS::SageMaker::CodeRepository	예	아니요	예	아니요
AWS::SageMaker::Domain	예	아니요	예	아니요

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::SageMaker::EndpointConfig	예	아니요	예	아니요
AWS::SageMaker::FeatureGroup	예	예	예	아니요
AWS::SageMaker::Image	예	예	예	예
AWS::SageMaker::InferenceExperiment	예	아니요	예	아니요
AWS::SageMaker::Model	예	아니요	예	아니요
AWS::SageMaker::NotebookInstance	예	아니요	예	아니요
AWS::SageMaker::NotebookInstanceLifecycleConfig	예	아니요	예	아니요
AWS::SecretsManager::Secret	예	예	예	예
AWS::SecurityHub::Standard	예	예	예	예
AWS::ServiceCatalog::CloudFormationProduct	예	아니요	예	예
AWS::ServiceCatalog::CloudFormationProvisionedProduct	예	아니요	예	예
AWS::ServiceCatalog::Portfolio	예	아니요	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::ServiceDiscovery::HttpNamespace	예	예	예	예
AWS::ServiceDiscovery::Instance	예	아니요	예	예
AWS::ServiceDiscovery::PublicDnsNamespace	예	예	예	예
AWS::ServiceDiscovery::Service	예	아니요	예	예
AWS::ShieldRegional::Protection	예	아니요	예	예
AWS::Signer::SigningProfile	예	아니요	예	아니요
AWS::StepFunctions::Activity	예	예	예	예
AWS::StepFunctions::StateMachine	예	예	예	예
AWS::Transfer::Agreement	예	아니요	예	예
AWS::Transfer::Certificate	예	예	예	예
AWS::Transfer::Connector	예	예	예	예
AWS::Transfer::Profile	예	예	예	예

리소스 유형	아프리카(케이프타운)	이스라엘(텔아비브)	중동(바레인)	중동(UAE)
AWS::Transfer::Workflow	예	예	예	예
AWS::WAFRegional::RateBasedRule	예	예	예	예
AWS::WAFRegional::Rule	예	예	예	예
AWS::WAFRegional::RuleGroup	예	예	예	예
AWS::WAFRegional::WebACL	예	예	예	예
AWS::WAFv2::IPSet	예	예	예	예
AWS::WAFv2::ManagedRuleSet	예	예	예	예
AWS::WAFv2::RegexPatternSet	예	예	예	예
AWS::WAFv2::RuleGroup	예	예	예	예
AWS::WAFv2::WebACL	예	예	예	예
AWS::WorkSpaces::Workspace	예	아니요	아니요	아니요
AWS::XRay::EncryptionConfig	예	예	아니요	예

GovCloud 리전

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::ACM::Certificate	예	예
AWS::ACMPCA::CertificateAuthority	예	예
AWS::ACMPCA::CertificateAuthorityActivation	예	예
AWS::AccessAnalyzer::Analyzer	예	예
AWS::AmazonMQ::Broker	예	예
AWS::ApiGateway::RestApi	예	예
AWS::ApiGateway::Stage	예	예
AWS::ApiGatewayV2::Api	예	예
AWS::ApiGatewayV2::Stage	예	예
AWS::AppConfig::Application	예	예
AWS::AppConfig::ConfigurationProfile	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::AppConfig::DeploymentStrategy	예	예
AWS::AppConfig::Environment	예	예
AWS::AppConfig::ExtensionAssociation	예	예
AWS::AppConfig::HostedConfigurationVersion	예	예
AWS::AppStream::Application	예	예
AWS::AppStream::DirectoryConfig	예	아니요
AWS::AppStream::Fleet	예	아니요
AWS::AppStream::Stack	예	아니요
AWS::Athena::DataCatalog	예	예
AWS::Athena::WorkGroup	예	예
AWS::AutoScaling::AutoScalingGroup	예	예
AWS::AutoScaling::LaunchConfiguration	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::AutoScaling::ScalingPolicy	예	예
AWS::AutoScaling::ScheduledAction	예	예
AWS::AutoScaling::WarmPool	예	예
AWS::Backup::BackupPlan	예	예
AWS::Backup::BackupSelection	예	예
AWS::Backup::BackupVault	예	예
AWS::Backup::RecoveryPoint	예	예
AWS::Batch::ComputeEnvironment	예	예
AWS::Batch::JobQueue	예	예
AWS::Batch::SchedulingPolicy	예	예
AWS::Bedrock::Guardrail	예	예
AWS::Bedrock::KnowledgeBase	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::Cassandra::Keyspace	예	예
AWS::CloudFormation::Stack	예	예
AWS::CloudTrail::Trail	예	예
AWS::CloudWatch::Alarm	예	예
AWS::CodeBuild::Project	예	예
AWS::CodeBuild::ReportGroup	예	예
AWS::Cognito::IdentityPool	예	아니요
AWS::Cognito::UserPoolGroup	예	아니요
AWS::Config::ConfigurationRecorder	예	예
AWS::Config::ConformancePackCompliance	예	예
AWS::Config::ResourceCompliance	예	예
AWS::Connect::Instance	예	아니요

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::Connect::QuickConnect	예	아니요
AWS::Connect::User	예	아니요
AWS::DMS::Certificate	예	예
AWS::DMS::Endpoint	예	예
AWS::DMS::EventSubscription	예	예
AWS::DMS::ReplicationInstance	예	예
AWS::DMS::ReplicationSubnetGroup	예	예
AWS::DMS::ReplicationTask	예	예
AWS::DataSync::LocationEFS	예	예
AWS::DataSync::LocationFSxLustre	예	예
AWS::DataSync::LocationFSxWindows	예	예
AWS::DataSync::LocationHDFS	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::DataSync::LocationNFS	예	예
AWS::DataSync::LocationObjectStorage	예	예
AWS::DataSync::LocationS3	예	예
AWS::DataSync::LocationSMB	예	예
AWS::DataSync::Task	예	예
AWS::Detective::Graph	예	예
AWS::DynamoDB::Table	예	예
AWS::EC2::CapacityReservation	예	예
AWS::EC2::ClientVpnEndpoint	예	예
AWS::EC2::ClientVpnTargetNetworkAssociation	예	예
AWS::EC2::CustomerGateway	예	예
AWS::EC2::DHCPOptions	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::EC2::EC2Fleet	예	예
AWS::EC2::EIP	예	예
AWS::EC2::EgressOnlyInternetGateway	예	예
AWS::EC2::FlowLog	예	예
AWS::EC2::Host	예	예
AWS::EC2::IPAM	예	예
AWS::EC2::IPAMPool	예	예
AWS::EC2::IPAMResourceDiscovery	예	예
AWS::EC2::IPAMResourceDiscoveryAssociation	예	예
AWS::EC2::IPAMScope	예	예
AWS::EC2::Instance	예	예
AWS::EC2::InstanceConnectEndpoint	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::EC2::InternetGateway	예	예
AWS::EC2::LaunchTemplate	예	예
AWS::EC2::NatGateway	예	예
AWS::EC2::NetworkAcl	예	예
AWS::EC2::NetworkInterface	예	예
AWS::EC2::PrefixList	예	예
AWS::EC2::RouteTable	예	예
AWS::EC2::SecurityGroup	예	예
AWS::EC2::SnapshotBlockPublicAccess	예	예
AWS::EC2::SpotFleet	예	예
AWS::EC2::Subnet	예	예
AWS::EC2::SubnetRouteTableAssociation	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::EC2::TrafficMirrorFilter	예	예
AWS::EC2::TrafficMirrorSession	예	예
AWS::EC2::TrafficMirrorTarget	예	예
AWS::EC2::TransitGateway	예	아니요
AWS::EC2::TransitGatewayAttachment	예	예
AWS::EC2::TransitGatewayConnect	예	예
AWS::EC2::TransitGatewayMulticastDomain	예	예
AWS::EC2::TransitGatewayRouteTable	예	예
AWS::EC2::VPC	예	예
AWS::EC2::VPCBlockPublicAccessExclusion	예	예
AWS::EC2::VPCBlockPublicAccessOptions	예	예
AWS::EC2::VPCEndpoint	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::EC2::VPCEndpointConnectionNotification	예	예
AWS::EC2::VPCEndpointService	예	아니요
AWS::EC2::VPCPeeringConnection	예	예
AWS::EC2::VPNConnection	예	예
AWS::EC2::VPNConnectionRoute	예	예
AWS::EC2::VPNGateway	예	예
AWS::EC2::Volume	예	예
AWS::ECR::Repository	예	예
AWS::ECS::CapacityProvider	예	예
AWS::ECS::Cluster	예	예
AWS::ECS::Service	예	예
AWS::ECS::TaskDefinition	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::ECS::TaskSet	예	예
AWS::EFS::AccessPoint	예	예
AWS::EFS::FileSystem	예	예
AWS::EKS::Addon	예	예
AWS::EKS::Cluster	예	예
AWS::EKS::IdentityProviderConfig	예	예
AWS::EMR::SecurityConfiguration	예	예
AWS::ElasticBeanstalk::Application	예	예
AWS::ElasticBeanstalk::ApplicationVersion	예	예
AWS::ElasticBeanstalk::Environment	예	예
AWS::ElasticLoadBalancing::LoadBalancer	예	예
AWS::ElasticLoadBalancingV2::Listener	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::ElasticLoadBalancingV2::LoadBalancer	예	예
AWS::Elasticsearch::Domain	예	예
AWS::Events::EventBus	예	예
AWS::Events::Rule	예	예
AWS::FIS::ExperimentTemplate	예	예
AWS::Glue::Classifier	예	예
AWS::Glue::Job	예	예
AWS::Glue::MLTransform	예	아니요
AWS::GreengrassV2::ComponentVersion	예	예
AWS::GuardDuty::Detector	예	예
AWS::GuardDuty::Filter	예	예
AWS::GuardDuty::IPSet	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::GuardDuty::ThreatIntelSet	예	예
AWS::IAM::Group	예	예
AWS::IAM::InstanceProfile	아니요	예
AWS::IAM::OIDCProvider	아니요	예
AWS::IAM::Policy	예	예
AWS::IAM::Role	예	예
AWS::IAM::SAMLProvider	아니요	예
AWS::IAM::ServerCertificate	아니요	예
AWS::IAM::User	예	예
AWS::ImageBuilder::ContainerRecipe	예	예
AWS::ImageBuilder::DistributionConfiguration	예	예
AWS::ImageBuilder::ImagePipeline	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::ImageBuilder::ImageRecipe	예	예
AWS::ImageBuilder::InfrastructureConfiguration	예	예
AWS::InspectorV2::Activation	예	예
AWS::IoT::AccountAuditConfiguration	예	예
AWS::IoT::Authorizer	예	예
AWS::IoT::CACertificate	예	예
AWS::IoT::CustomMetric	예	예
AWS::IoT::Dimension	예	예
AWS::IoT::FleetMetric	예	예
AWS::IoT::JobTemplate	예	예
AWS::IoT::MitigationAction	예	예
AWS::IoT::Policy	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::IoT::ProvisioningTemplate	예	예
AWS::IoT::RoleAlias	예	예
AWS::IoT::ScheduledAudit	예	예
AWS::IoT::SecurityProfile	예	예
AWS::IoTEvents::AlarmModel	예	아니요
AWS::IoTEvents::DetectorModel	예	아니요
AWS::IoTEvents::Input	예	아니요
AWS::IoTSiteWise::AssetModel	예	아니요
AWS::IoTSiteWise::Gateway	예	아니요
AWS::IoTSiteWise::Portal	예	아니요
AWS::IoTTwinMaker::ComponentType	예	아니요
AWS::IoTTwinMaker::Entity	예	아니요

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::IoTTwinMaker::Workspace	예	아니요
AWS::KMS::Alias	예	예
AWS::KMS::Key	예	예
AWS::Kinesis::Stream	예	예
AWS::Kinesis::StreamConsumer	예	예
AWS::KinesisAnalyticsV2::Application	예	예
AWS::KinesisFirehose::DeliveryStream	예	예
AWS::Lambda::Function	예	예
AWS::Logs::Destination	예	예
AWS::MSK::BatchScramSecret	예	예
AWS::MSK::Cluster	예	예
AWS::MSK::ClusterPolicy	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::MSK::Configuration	예	예
AWS::MSK::VpcConnection	예	예
AWS::NetworkFirewall::Firewall	예	예
AWS::NetworkFirewall::FirewallPolicy	예	예
AWS::NetworkFirewall::RuleGroup	예	예
AWS::NetworkFirewall::VpcEndpointAssociation	예	예
AWS::NetworkManager::CustomerGatewayAssociation	예	아니요
AWS::NetworkManager::Device	예	아니요
AWS::NetworkManager::GlobalNetwork	예	아니요
AWS::NetworkManager::Link	예	아니요
AWS::NetworkManager::LinkAssociation	예	아니요
AWS::NetworkManager::Site	예	아니요

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::NetworkManager::TransitGatewayRegistration	예	아니요
AWS::OpenSearch::Domain	예	예
AWS::Pinpoint::App	예	아니요
AWS::Pinpoint::ApplicationSettings	예	아니요
AWS::Pinpoint::Campaign	예	아니요
AWS::Pinpoint::EmailChannel	예	아니요
AWS::Pinpoint::EmailTemplate	예	아니요
AWS::Pinpoint::EventStream	예	아니요
AWS::Pinpoint::InAppTemplate	예	아니요
AWS::Pinpoint::Segment	예	아니요
AWS::QuickSight::Template	예	아니요
AWS::RDS::DBCluster	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::RDS::DBClusterSnapshot	예	예
AWS::RDS::DBInstance	예	예
AWS::RDS::DBSecurityGroup	예	예
AWS::RDS::DBSnapshot	예	예
AWS::RDS::DBSubnetGroup	예	예
AWS::RDS::EventSubscription	예	예
AWS::RDS::OptionGroup	예	예
AWS::Redshift::Cluster	예	예
AWS::Redshift::ClusterParameterGroup	예	예
AWS::Redshift::ClusterSecurityGroup	예	예
AWS::Redshift::ClusterSnapshot	예	예
AWS::Redshift::ClusterSubnetGroup	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::Redshift::EventSubscription	예	예
AWS::Redshift::ScheduledAction	예	예
AWS::RoboMaker::RobotApplication	예	아니요
AWS::RoboMaker::RobotApplicationVersion	예	아니요
AWS::RoboMaker::SimulationApplication	예	아니요
AWS::Route53Profiles::Profile	예	예
AWS::Route53Resolver::FirewallDomainList	예	예
AWS::Route53Resolver::FirewallRuleGroup	예	예
AWS::Route53Resolver::FirewallRuleGroupAssociation	예	예
AWS::Route53Resolver::ResolverEndpoint	예	예
AWS::Route53Resolver::ResolverQueryLoggingConfig	예	예
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::Route53Resolver::ResolverRule	예	예
AWS::Route53Resolver::ResolverRuleAssociation	예	예
AWS::S3::AccessPoint	예	예
AWS::S3::AccountPublicAccessBlock	예	예
AWS::S3::Bucket	예	예
AWS::SES::ConfigurationSet	예	아니요
AWS::SES::ContactList	예	아니요
AWS::SES::Template	예	아니요
AWS::SNS::Topic	예	예
AWS::SQS::Queue	예	예
AWS::SSM::AssociationCompliance	예	예
AWS::SSM::Document	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::SSM::FileData	예	예
AWS::SSM::ManagedInstanceInventory	예	예
AWS::SSM::PatchCompliance	예	예
AWS::SageMaker::Model	예	아니요
AWS::SageMaker::NotebookInstance	예	아니요
AWS::SageMaker::NotebookInstanceLifecycleConfig	예	아니요
AWS::SecretsManager::Secret	예	예
AWS::SecurityHub::Standard	예	예
AWS::ServiceCatalog::CloudFormationProduct	예	예
AWS::ServiceCatalog::CloudFormationProvisionedProduct	예	예
AWS::ServiceCatalog::Portfolio	예	예
AWS::ServiceDiscovery::HttpNamespace	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::ServiceDiscovery::Instance	예	예
AWS::ServiceDiscovery::Service	예	예
AWS::StepFunctions::StateMachine	예	예
AWS::Transfer::Agreement	예	예
AWS::Transfer::Certificate	예	예
AWS::Transfer::Connector	예	예
AWS::Transfer::Profile	예	예
AWS::Transfer::Workflow	예	예
AWS::WAFRegional::RateBasedRule	예	예
AWS::WAFRegional::Rule	예	예
AWS::WAFRegional::RuleGroup	예	예
AWS::WAFRegional::WebACL	예	예

리소스 유형	AWS GovCloud(미국 서부)	AWS GovCloud(미국 동부)
AWS::WAFv2::IPSet	예	예
AWS::WAFv2::ManagedRuleSet	예	예
AWS::WAFv2::RegexPatternSet	예	예
AWS::WAFv2::RuleGroup	예	예
AWS::WAFv2::WebACL	예	예
AWS::WorkSpaces::Workspace	예	아니요

를 사용하여 AWS 리소스 기록 AWS Config

AWS Config 는 지원되는 리소스 유형이 생성, 변경 또는 삭제되는 시기를 지속적으로 감지합니다.는 이러한 이벤트를 구성 항목(CIs)으로 AWS Config 기록합니다.

지원되는 모든 리소스 유형 또는 사용자와 관련된 지원되는 리소스 유형에 대해서만 구성 변경을 기록 AWS Config 하도록를 사용자 지정할 수 있습니다. 에서 기록할 AWS Config 수 있는 지원되는 리소스 유형 목록은 섹션을 참조하세요에 대해 지원되는 리소스 유형 AWS Config.

주제

- 고려 사항
- 리전 리소스와 글로벌 리소스의 차이점
- AWS Config 규칙 및 글로벌 리소스 유형
- 의 레코딩 빈도 AWS Config
- 기록되지 않은 리소스

- AWS Config 콘솔에서 리소스 기록
- AWS CLI를 사용하여 리소스 기록
- 를 사용한 레코딩에서 리소스 제외 AWS Config
- 고객 관리형 구성 레코더를 사용한 AWS Config 레코딩 중지

고려 사항

높은 AWS Config 평가 수

다음 달과 비교할 때 AWS Config를 사용하여 처음 한 달을 기록하는 동안 계정에서 활동이 증가하는 것을 확인할 수 있습니다. 초기 부트스트래핑 프로세스 중에는가 기록 AWS Config 하도록 선택한 계정의 모든 리소스에 대한 평가를 AWS Config 실행합니다.

임시 워크로드를 실행하는 경우 이러한 임시 리소스 생성 및 삭제와 관련된 구성 변경을 기록 AWS Config 하므로의 활동이 증가할 수 있습니다. 임시 워크로드는 컴퓨팅 리소스를 필요할 때 로드 및 실행하는 일시적 사용입니다. 대표적인 예는 Amazon Elastic Compute Cloud(Amazon EC2) 스팟 인스턴스, Amazon EMR 작업, AWS Auto Scaling이 있습니다.

증가된 활동이 임시 워크로드를 실행하지 않도록 하려면 이러한 리소스 유형이 기록되지 않도록 고객 관리형 구성 레코더를 설정하거나가 꺼 AWS Config 진 별도의 계정에서 이러한 유형의 워크로드를 실행하여 구성 기록 및 규칙 평가가 증가하지 않도록 할 수 있습니다.

리전 가용성

추적할 리소스 유형을 지정 AWS Config 하기 전에 리전 가용성별 리소스 적용 범위를 확인하여 설정한 AWS 리전에서 리소스 유형이 지원되는지 확인합니다 AWS Config.

리소스 유형이 하나 이상의 리전 AWS Config 에서에서 지원되는 경우, 설정한 리전에서 AWS Config 지정된 리소스 유형이 지원되지 않더라도에서 지원하는 모든 AWS 리전에서 해당 리소스 유형의 기록을 활성화할 수 있습니다 AWS Config.

리전 리소스와 글로벌 리소스의 차이점

리전 리소스

리전 리소스는 한 리전에 한정되어 있으며 해당 리전에서만 사용할 수 있습니다. 지정된에서 생성한 AWS 리전다음 해당 리전에 존재합니다. 이러한 리소스를 보거나 해당 리소스와 상호 작용하려면 해당 리전으로 작업을 지시해야 합니다. 예를 들어를 사용하여 Amazon EC2 인스턴스를 생성하려면 인스턴스를 생성할를 AWS Management Console선택합니다 AWS 리전. AWS Command

Line Interface (AWS CLI)를 사용하여 인스턴스를 생성하는 경우 `--region` 파라미터를 포함합니다. 각 AWS SDKs에는 작업이 사용하는 리전을 지정하는 것과 동일한 자체 메커니즘이 있습니다.

리전 리소스를 사용하는 데에는 여러 가지 이유가 있습니다. 한 가지 이유는 리소스와 리소스 액세스에 사용하는 서비스 엔드포인트가 고객과 가능한 한 가까운 곳에 위치하도록 보장하는 것입니다. 그러면 지연 시간이 최소화되어 성능이 향상됩니다. 또 다른 이유는 격리 경계를 제공하기 위해서입니다. 이를 통해 리소스의 독립적인 복사본을 여러 리전에 생성하여 부하를 분산하고 확장성을 개선할 수 있습니다. 동시에 리소스를 서로 분리하여 가용성을 높일 수 있습니다.

콘솔이나 AWS CLI 명령 AWS 리전 에서 다른를 지정하면 더 이상 이전 리전에서 볼 수 있는 리소스를 보거나 상호 작용할 수 없습니다.

리전 리소스의 Amazon 리소스 이름(ARN)을 보면 해당 리소스가 포함된 리전이 ARN의 네 번째 필드로 지정되어 있습니다. 예를 들어 Amazon EC2 인스턴스는 리전 리소스입니다. 다음은 `us-east-1` 리전의 Amazon EC2 인스턴스에 대한 ARN의 예입니다.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

글로벌 리소스

일부 AWS 서비스 리소스는 글로벌 리소스이므로 어디서나 리소스를 사용할 수 있습니다. 글로벌 서비스의 콘솔에서는 AWS 리전 을 지정하지 않습니다. 글로벌 리소스에 액세스하려면 서비스의 AWS CLI 및 AWS SDK 작업을 사용할 때 `--region` 파라미터를 지정하지 않습니다.

글로벌 리소스는 특정 리소스의 인스턴스가 한 번에 하나만 있어야 하는 경우를 지원합니다. 이러한 경우 서로 다른 리전에 있는 복사본 간 복제 또는 동기화는 바람직하지 않습니다. 단일 글로벌 엔드포인트에 액세스하는 것은 지연 시간이 늘어날 수는 있지만, 모든 변경 사항을 리소스 소비자에게 즉시 표시할 수 있다는 점에서 허용 가능한 것으로 간주됩니다.

예를 들어 Amazon Aurora 글로벌 클러스터(`AWS::RDS::GlobalCluster`)는 글로벌 리소스이므로 특정 리전에 연결되지 않습니다. 즉, 리전 엔드포인트에 의존하지 않고도 글로벌 클러스터를 생성할 수 있습니다. 그러면 Amazon Relational Database Service(RDS) 자체는 리전별로 구성되어 있지만 글로벌 클러스터가 시작된 특정 지역은 글로벌 클러스터에 영향을 미치지 않는다는 이점이 있습니다. 따라서 모든 리전에서 하나의 연속적인 글로벌 네트워크로 나타납니다.

글로벌 리소스의 Amazon 리소스 이름(ARN)에는 리전이 포함되지 않습니다. 아래의 글로벌 클러스터의 ARN 예에서 볼 수 있듯이 네 번째 필드는 비어 있습니다.

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> 2022년 2월 AWS Config 이후에 온보딩된 글로벌 리소스 유형은 상용 파티션의 경우 서비스의 홈 리전에, GovCloud AWS 파티션의 경우 GovCloud(미국 서부)에만 기록됩니다. 이러한 새 글로벌 리소스 유형에 대한 구성 항목(CIs 홈 리전 및 AWS GovCloud(미국 서부)에서만 볼 수 있습니다.
> 2022년 2월 이전에 온보딩된 글로벌 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role`, `AWS::IAM::User`)은 변경되지 않습니다. 2022년 2월 이전에가 지원되는 모든 리전에서 이러한 글로벌 IAM 리소스의 기록을 활성화할 수 AWS Config 있습니다. 이러한 글로벌 IAM 리소스는 2022년 2월 AWS Config 이후에서 지원하는 리전에 기록할 수 없습니다.

글로벌 리소스 유형 | IAM 리소스

다음 IAM 리소스 유형도 글로벌 리소스입니다. IAM 사용자, 그룹, 역할 및 고객 관리형 정책. 이러한 리소스 유형은가 2022년 2월 이전에 사용 가능한 리전에서에 의해 AWS Config 기록될 수 AWS Config 있습니다. 글로벌 IAM 리소스 유형을 기록할 수 없는이 목록에는 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 아시아 태평양(태국), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히), 이스라엘(텔아비브), 멕시코(중부), 중동(UAE) 리전이 포함됩니다.

구성 항목(CI) 중복을 방지하려면 한 번에 지원되는 리전 중 하나에서만 글로벌 IAM 리소스 유형을 기록하는 것이 좋습니다. 또한 이를 통해 불필요한 평가 및 API 제한을 피할 수 있습니다.

글로벌 리소스 유형 | 홈 리전만 해당

다음 서비스에 대한 글로벌 리소스는 Amazon Elastic Container Registry Public, Amazon Route 53 AWS Global Accelerator, Amazon CloudFront 및 글로벌 리소스 유형의 홈 리전에서만 AWS Config 에 의해 기록됩니다 AWS WAF. 이러한 글로벌 리소스의 경우 리소스 유형의 동일한 인스턴스를 여러 AWS 리전에서 사용할 수 있지만 구성 항목(CIs)은 상용 파티션의 홈 리전 또는 AWS GovCloud (US) 파티션의 AWS GovCloud(미국 서부)에만 기록됩니다.

글로벌 리소스 유형의 홈 리전

AWS 서비스	리소스 유형 값	홈 리전
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	미국 동부(버지니아 북부) 리전

AWS 서비스	리소스 유형 값	홈 리전
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	US West (Oregon) Region
	`AWS::GlobalAccelerator::EndpointGroup`	US West (Oregon) Region
	`AWS::GlobalAccelerator::Accelerator`	US West (Oregon) Region
Amazon Route 53	`AWS::Route53::HostedZone`	미국 동부(버지니아 북부) 리전
	`AWS::Route53::HealthCheck`	미국 동부(버지니아 북부) 리전
Amazon CloudFront	`AWS::CloudFront::Distribution`	미국 동부(버지니아 북부) 리전
AWS WAF	`AWS::WAFv2::WebACL`	미국 동부(버지니아 북부) 리전

글로벌 리소스 유형 | Aurora 글로벌 클러스터

`AWS::RDS::GlobalCluster`는 고객 관리형 구성 레코더가 활성화된 지원되는 모든 AWS Config 리전에 기록되는 글로벌 리소스입니다. 이 글로벌 리소스 유형은 한 리전에서이 리소스의 기록을 활성화하면가 활성화된 모든 리전에서이 리소스 유형에 대한 구성 항목(CIs)을 AWS Config 기록한다는 점에서 고유합니다.

활성화된 모든 리전에서 `AWS::RDS::GlobalCluster`를 기록하지 않으려면 AWS Config 콘솔에서 다음 기록 전략 중 하나를 사용하세요.

- 사용자 지정 가능한 재정의가 있는 모든 리소스 유형을 기록하고 "AWS RDS GlobalCluster"를 선택한 다음 "레코딩에서 제외"를 선택합니다.
- 특정 리소스 유형을 기록.

활성화된 모든 리전에서 `AWS::RDS::GlobalCluster`를 기록하지 않으려면 API/CLI에서 다음 기록 전략 중 하나를 사용하세요.

- 제외 항목 이외의 모든 현재 및 향후 리소스 유형을 기록(`EXCLUSION_BY_RESOURCE_TYPES`)
- 특정 리소스 유형을 기록(`INCLUSION_BY_RESOURCE_TYPES`).

AWS Config 규칙 및 글로벌 리소스 유형

2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사용 가능한 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 글로벌 IAM 리소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에 기록할 수 없습니다. 해당 리전 목록은 AWS 리소스 레코딩 | 글로벌 리소스 페이지를 참조하세요.

주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.

2022년 2월 이전 온보딩한 글로벌 리소스에 대한 규정 준수 보고 모범 사례

불필요한 평가를 방지하려면 이러한 글로벌 리소스 범위가 있는 AWS Config 규칙 및 적합성 팩만 지원되는 리전 중 하나에 배포해야 합니다. 어떤 리전에서 어떤 관리형 규칙이 지원되는지 목록을 보려면 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요. 이는 AWS Config 규칙, 조직 AWS Config 규칙 및 AWS Security Hub 및와 같은 다른 AWS 서비스에서 생성한 규칙에도 적용됩니다 AWS Control Tower.

2022년 2월 이전에 온보딩된 글로벌 리소스 유형을 기록하지 않는 경우, 불필요한 평가가 발생하지 않도록 다음 주기적 규칙을 활성화하지 않는 것이 좋습니다.

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check

- mfa-enabled-for-iam-console-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

2022년 2월 이후 온보딩한 글로벌 리소스에 대한 규정 준수 보고 모범 사례

2022년 2월 이후에 AWS Config 기록에 온보딩된 글로벌 리소스 유형은 상용 파티션의 경우 서비스의 홈 리전에, AWS GovCloud (US) 파티션의 경우 AWS GovCloud(미국 서부)에만 기록됩니다. 이러한 글로벌 리소스의 범위가 인 AWS Config 규칙 및 적합성 팩은 리소스 유형의 홈 리전에만 배포해야 합니다. 자세한 내용은 글로벌 리소스 유형의 홈 리전을 참조하세요.

의 레코딩 빈도 AWS Config

AWS Config 는 연속 레코딩 및 일일 레코딩을 지원합니다. 지속적인 기록을 사용하면 변경이 발생할 때마다 지속적으로 구성 변경 사항을 기록할 수 있습니다. 일일 기록을 사용하면 이전에 기록된 CI와 다른 경우에만 지난 24시간 동안의 리소스 최신 상태를 나타내는 구성 항목(CI)을 받을 수 있습니다. 레코딩 빈도를 변경하는 방법에 대한 단계는 레코딩 빈도 변경을 참조하세요.

지속적인 기록

지속적인 기록의 몇 가지 이점은 다음과 같습니다.

- 실시간 모니터링: 지속적인 기록을 통해 무단 변경이나 예상치 못한 변경을 즉시 탐지하여 보안 및 규정 준수 노력을 강화할 수 있습니다.
- 세부 분석: 지속적인 기록을 통해 리소스의 구성 변경 발생 시 심층 분석을 수행할 수 있으며, 이를 통해 순간의 패턴과 추세를 식별할 수 있습니다.

일일 기록

일일 기록의 몇 가지 이점은 다음과 같습니다.

- 방해 최소화: 일일 기록은 보다 관리하기 용이한 정보 흐름을 제공하며 알림 빈도와 경고 피로를 줄일 수 있습니다.
- 비용 효율성: 일일 기록은 더 낮은 빈도로 리소스에 대한 변경 사항을 기록할 수 있는 유연성을 제공하여 기록된 구성 변경 횟수와 관련된 비용을 줄일 수 있습니다.

> **Note**
>
> AWS Firewall Manager 는 리소스를 모니터링하기 위해 지속적인 레코딩에 의존합니다. Firewall Manager를 사용하는 경우 기록 빈도를 계속으로 설정하는 것이 좋습니다.

기록되지 않은 리소스

리소스가 기록되지 않은 경우는 무료로 해당 리소스의 생성 및 삭제만 캡처하고 다른 세부 정보는 AWS Config 캡처하지 않습니다. 레코딩되지 않은 리소스가 생성되거나 삭제되면가 알림을 AWS Config 보내고 리소스 세부 정보 페이지에 이벤트를 표시합니다. 기록되지 않는 리소스의 세부 정보 페이지는 대부분의 구성 세부 정보에 대해 null 값을 표시하며, 관계 및 구성 변경에 대한 정보는 제공하지 않습니다.

가 기록된 리소스에 AWS Config 대해 제공하는 관계 정보는 기록되지 않은 리소스에 대한 데이터가 누락되었기 때문에 제한되지 않습니다. 기록된 리소스가 기록되지 않은 리소스와 관련이 있는 경우, 기록된 리소스의 세부 정보 페이지에 해당 관계가 제공됩니다.

IAM 리소스 유형 고려 사항

`AWS::IAM::User`, `AWS::IAM::Policy` `AWS::IAM::Group`, `AWS::IAM::Role` 리소스 유형은 리소스가 고객 관리형 구성 레코더에 기록할 리소스로 선택되었거나 이전에 선택된 경우에만 생성(`ResourceNotRecorded`) 및 삭제(`ResourceDeletedNotRecorded`) 상태를 캡처합니다.

기록되지 않은 리소스에 대한 CI 기록 일정

`ResourceNotRecorded` 및 `ResourceDeletedNotRecorded`의 구성 항목(CI)은 리소스 유형에 대한 일반적인 기록 시간을 따르지 않습니다. 이러한 리소스 유형은 고객 관리형 구성 레코더의 주기적 기준 설정 프로세스 중에만 기록되며, 다른 리소스 유형보다 빈도가 낮습니다. 즉, 생성 또는 삭제 시 알림 생성 및 삭제가 전송되지 않고 기준 설정 프로세스 중에 전송됩니다.

CI 전송 및 서비스 연결 레코더 범위

서비스 연결 구성 레코더의 경우 기록 범위에 따라 전송 채널에서 구성 항목(CIs)을 수신할지 여부가 결정됩니다. 기록 범위는 구성 레코더에 연결된 서비스에 의해 설정됩니다. 기록 범위가 내부인 경우 전송 채널에서 CIs를 수신하지 않습니다.

AWS Config 콘솔에서 리소스 기록

AWS Config 콘솔을 사용하여가 고객 관리형 구성 레코더로 AWS Config 기록하는 리소스 유형을 선택할 수 있습니다.

리소스를 선택하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 설정을 선택합니다.
3. 고객 관리형 레코더 탭에서 편집을 선택합니다.
4. 기록 방법 섹션에서 기록 전략을 선택합니다. 기록할 AWS 리소스를 지정할 수 AWS Config 있습니다.

   All resource types with customizable overrides

   이 리전에서 현재 및 향후 지원되는 모든 리소스 유형에 대한 구성 변경을 기록 AWS Config 하도록 설정합니다. 특정 리소스 유형의 기록 빈도를 재정의하거나 기록에서 특정 리소스 유형을 제외할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.

   - 기본 설정

     현재 및 향후 지원되는 모든 리소스 유형에 대한 기본 기록 빈도를 구성합니다. 자세한 내용은 기록 빈도를 참조하세요.

     - 연속 기록 - 변경 AWS Config 사항이 발생할 때마다 구성 변경을 지속적으로 기록합니다.
     - 일일 기록 - 이전에 기록된 CI와 다른 경우에만 지난 24시간 동안의 리소스 최신 상태를 나타내는 구성 항목(CI)을 받게 됩니다.

     > **Note**
     >
     > AWS Firewall Manager 는 리소스를 모니터링하기 위해 지속적인 레코딩에 의존합니다. Firewall Manager를 사용하는 경우 기록 빈도를 계속으로 설정하는 것이 좋습니다.

   - 설정 재정의

     특정 리소스 유형의 기록 빈도를 재정의하거나 기록에서 특정 리소스 유형을 제외합니다. 리소스 유형의 기록 빈도를 변경하거나 리소스 유형에 대한 기록을 중지하는 경우 이미 기록된 구성 항목은 변경되지 않습니다.

   Specific resource types

   지정한 리소스 유형에 대해서만 구성 변경을 기록 AWS Config 하도록를 설정합니다.

- 특정 리소스 유형

  기록할 리소스 유형과 빈도를 선택합니다. 자세한 내용은 기록 빈도를 참조하세요.

  - 연속 기록 - 변경 AWS Config 사항이 발생할 때마다 구성 변경을 지속적으로 기록합니다.
  - 일일 기록 - 이전에 기록된 CI와 다른 경우에만 지난 24시간 동안의 리소스 최신 상태를 나타내는 구성 항목(CI)을 받게 됩니다.

  > **Note**
  >
  > AWS Firewall Manager 는 리소스를 모니터링하기 위해 지속적인 레코딩에 의존합니다. Firewall Manager를 사용하는 경우 기록 빈도를 계속으로 설정하는 것이 좋습니다.

  리소스 유형의 기록 빈도를 변경하거나 리소스 유형에 대한 기록을 중지하는 경우 이미 기록된 구성 항목은 변경되지 않습니다.

5. 저장을 선택하여 변경 사항을 저장합니다.

리소스 기록 시 고려 사항

높은 AWS Config 평가 수

다음 달과 비교할 때 AWS Config를 사용하여 처음 한 달을 기록하는 동안 계정에서 활동이 증가하는 것을 확인할 수 있습니다. 초기 부트스트래핑 프로세스 중에는가 기록 AWS Config 하도록 선택한 계정의 모든 리소스에 대한 평가를 AWS Config 실행합니다.

임시 워크로드를 실행하는 경우 이러한 임시 리소스 생성 및 삭제와 관련된 구성 변경을 기록 AWS Config 하므로의 활동이 증가할 수 있습니다. 임시 워크로드는 컴퓨팅 리소스를 필요할 때 로드 및 실행하는 일시적 사용입니다. 예를 들면 Amazon Elastic Compute Cloud(Amazon EC2) 스팟 인스턴스, Amazon EMR 작업 및 등이 AWS Auto Scaling있습니다. 임시 워크로드 실행으로 인한 활동 증가를 방지하려면 이러한 리소스 유형이 기록되지 않도록 고객 관리형 구성 레코더를 설정하거나가 꺼 AWS Config 진 별도의 계정에서 이러한 유형의 워크로드를 실행하여 구성 기록 및 규칙 평가가 증가하지 않도록 할 수 있습니다.

Considerations: All resource types with customizable overrides

전역적으로 기록되는 리소스 유형 | Aurora 글로벌 클러스터는 처음에 기록에 포함됨

`AWS::RDS::GlobalCluster` 리소스 유형은 고객 관리형 구성 레코더가 활성화된 지원되는 모든 AWS Config 리전에 기록됩니다.

활성화된 모든 리전에서 `AWS::RDS::GlobalCluster`를 기록하지 않으려면 'AWS RDS GlobalCluster'를 선택하고 '기록에서 제외' 재정의를 선택합니다.

글로벌 리소스 유형 | IAM 리소스 유형은 처음에 기록에서 제외됨

글로벌 IAM 리소스 유형은 비용 절감을 위해 처음에 기록에서 제외됩니다. 이 번들에는 IAM 사용자, 그룹, 역할 및 고객 관리형 정책이 포함됩니다. 재정의를 제거하고 이러한 리소스를 기록에 포함하려면 제거를 선택합니다.

또한 글로벌 IAM 리소스 유형(`AWS::IAM::User`, `AWS::IAM::Role`, 및 `AWS::IAM::GroupAWS::IAM::Policy`)은 2022년 2월 AWS Config 이후에서 지원하는 리전에 기록할 수 없습니다. 해당 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.

Limits

최대 100개의 빈도 재정의와 600개의 제외 재정의를 추가할 수 있습니다.

다음과 같은 리소스 유형에는 일일 기록이 지원되지 않습니다.

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

리전 가용성

추적할 리소스 유형을 지정 AWS Config 하기 전에 리전 가용성별 리소스 적용 범위를 확인하여 설정한 AWS 리전에서 리소스 유형이 지원되는지 확인합니다 AWS Config. 리소스 유형이 하나 이상의 리전 AWS Config 에서에서 지원되는 경우, 설정한 리전에서 AWS Config지정된 리소스 유형이 지원되지 않더라도에서 지원하는 모든 AWS 리전에서 해당 리소스 유형의 기록을 활성화할 수 있습니다 AWS Config.

Limits

모든 리소스 유형의 빈도가 같으면 제한이 없습니다. 하나 이상의 리소스 유형이 계속으로 설정된 경우 일일 빈도를 사용하여 최대 100개의 리소스 유형을 추가할 수 있습니다.

다음과 같은 리소스 유형에는 일일 빈도가 지원되지 않습니다.

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

AWS CLI를 사용하여 리소스 기록

AWS CLI를 사용하여 기록할 리소스 유형을 선택할 수 AWS Config 있습니다. 이렇게 하려면 기록 그룹에서 지정하는 리소스 유형을 기록하는 고객 관리형 구성 레코더를 생성합니다. 기록 그룹에서 지원되는 모든 리소스 유형을 기록할지 아니면 특정 유형의 리소스를 포함 또는 제외할지 지정합니다.

Record all current and future supported resource types

이 리전에서 현재 및 향후 지원되는 모든 리소스 유형에 대한 구성 변경을 기록 AWS Config 하도록 설정합니다. 지원되는 리소스 유형 목록은 지원되는 리소스 유형을 참조하세요.

1. `put-configuration-recorder` 명령을 사용합니다.

   이 명령은 `--configuration-recorder` 및 `---recording-group` 필드를 사용합니다.

   ```
   $ aws configservice put-configuration-recorder \
   --configuration-recorder file://configurationRecorder.json \
   --recording-group file://recordingGroup.json
   ```

   `configuration-recorder` 필드

   `configurationRecorder.json` 파일이 `name`, `roleArn` 및 구성 레코더 (`recordingMode`)의 기본 기록 빈도를 지정합니다.

   ```
   {
     "name": "default",
     "roleARN": "arn:aws:iam::123456789012:role/config-role",
     "recordingMode": {
       "recordingFrequency": CONTINUOUS or DAILY,
       "recordingModeOverrides": [
           {
               "description": "Description you provide for the override",
               "recordingFrequency": CONTINUOUS or DAILY,
               "resourceTypes": [ Comma-separated list of resource types to include
    in the override ]
           }
   ```

```
    ]
  }
}
```

recording-group 필드

recordingGroup.json 파일은 기록되는 리소스 유형을 지정합니다.

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

이러한 필드에 대한 자세한 내용은 명령 참조put-configuration-recorder의 섹션을 참조하세요. AWS CLI

2. (선택 사항) 고객 관리형 구성 레코더에 원하는 설정이 있는지 확인하려면 다음 describe-configuration-recorders 명령을 사용합니다.

```
$ aws configservice describe-configuration-recorders
```

다음은 응답의 예입니다.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default"
            "recordingGroup": {
                "allSupported": true,
                "exclusionByResourceTypes": {
                     "resourceTypes": []
                },
                "includeGlobalResourceTypes": true,
                "recordingStrategy": {
                    "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
```

```
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types
 to include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record all current and future supported resources types excluding the types you specify

기록에서 제외 AWS Config 하도록 지정한 리소스 유형을 제외하고 글로벌 리소스 유형을 포함하여 현재 및 향후 지원되는 모든 리소스 유형에 대한 구성 변경을 기록하도록를 설정합니다.

리소스 유형에 대한 기록을 중지하도록 선택하면 이미 기록된 구성 항목은 변경되지 않습니다. 지원되는 리소스 유형 목록은 지원되는 리소스 유형을 참조하세요.

1. put-configuration-recorder 명령을 사용합니다.

   이 명령은 `--configuration-recorder` 및 `---recording-group` 필드를 사용합니다.

   ```
   $ aws configservice put-configuration-recorder \
   --configuration-recorder file://configurationRecorder.json \
   --recording-group file://recordingGroup.json
   ```

   `configuration-recorder` 필드

   `configurationRecorder.json` 파일이 `name`, `roleArn` 및 구성 레코더(`recordingMode`)의 기본 기록 빈도를 지정합니다.

   ```
   {
     "name": "default",
     "roleARN": "arn:aws:iam::123456789012:role/config-role",
     "recordingMode": {
       "recordingFrequency": CONTINUOUS or DAILY,
   ```

```
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

recording-group 필드

recordingGroup.json 파일은 AWS Config 기록할 리소스 유형을 지정합니다. 다음 예제exclusionByResourceTypes와 같이의 resourceTypes 필드에서 제외할 하나 이상의 리소스 유형을 전달합니다.

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
   "includeGlobalResourceTypes": false,
   "recordingStrategy": {
       "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },

}
```

이러한 필드에 대한 자세한 내용은 명령 참조put-configuration-recorder의 섹션을 참조하세요. AWS CLI

2. (선택 사항) 고객 관리형 구성 레코더에 원하는 설정이 있는지 확인하려면 다음 describe-configuration-recorders 명령을 사용합니다.

```
$ aws configservice describe-configuration-recorders
```

다음은 응답의 예입니다.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record specific resource types

지정한 리소스 유형에 대해서만 구성 변경을 기록 AWS Config 하도록 설정합니다.

리소스 유형에 대한 기록을 중지하도록 선택하면 이미 기록된 구성 항목은 변경되지 않습니다. 지원되는 리소스 유형 목록은 지원되는 리소스 유형을 참조하세요.

1. put-configuration-recorder 명령을 사용합니다.

   이 명령은 `--configuration-recorder` 및 `---recording-group` 필드를 사용합니다.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

configuration-recorder 필드

`configurationRecorder.json` 파일이 `name`, `roleArn` 및 구성 레코더(`recordingMode`)의 기본 기록 빈도를 지정합니다.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

recording-group 필드

`recordingGroup.json` 파일은 AWS Config 기록할 리소스 유형을 지정합니다. 다음 예제와 같이 `resourceTypes` 필드에서 제외할 하나 이상의 리소스 유형을 전달합니다.

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
```

```
    },
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
  ]
}
```

이러한 필드에 대한 자세한 내용은 명령 참조put-configuration-recorder의 섹션을 참조하세요. AWS CLI

2. (선택 사항) 고객 관리형 구성 레코더에 원하는 설정이 있는지 확인하려면 다음 describe-configuration-recorders 명령을 사용합니다.

```
$ aws configservice describe-configuration-recorders
```

다음은 응답의 예입니다.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": []
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
```

```
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

를 사용한 레코딩에서 리소스 제외 AWS Config

AWS Config 를 사용하면 인벤토리 추적 및 규정 준수 모니터링에서 특정 유형의 AWS 리소스를 제외하는 동시에 향후 추가될 리소스를 AWS Config포함하여 현재 사용 가능한 다른 모든 지원되는 리소스 유형을 추적할 수 있습니다. 이 기능을 사용하면 규정 준수 및 거버넌스 표준이 적용되는 중요 리소스에 집중할 수 있습니다.

Excluding resources (Console)

AWS 리소스 유형을 기록하지 않으려면 AWS Config 콘솔에 대해 다음 기록 전략 중 하나를 사용합니다.

- 사용자 지정 가능한 재정의 를 사용하여 모든 리소스 유형을 기록하고, 제외하려는 리소스 유형을 선택한 다음, 재정의 '기록에서 제외'를 선택합니다.
- 특정 리소스 유형을 기록.

자세한 단계는 리소스 기록(콘솔)을 참조하세요.

Excluding resources (AWS CLI)

AWS 리소스 유형을 기록하지 않으려면 API/CLI에 대해 다음 기록 전략 중 하나를 사용합니다.

- 제외 항목 이외의 모든 현재 및 향후 리소스 유형을 기록(`EXCLUSION_BY_RESOURCE_TYPES`)
- 특정 리소스 유형을 기록(`INCLUSION_BY_RESOURCE_TYPES`).

자세한 단계는 리소스 기록(AWS CLI)을 참조하세요.

고객 관리형 구성 레코더를 사용한 AWS Config 레코딩 중지

언제든지 AWS Config 에서 고객 관리형 구성 레코더로 레코딩을 중지할 수 있습니다. 가 리소스 기록을 AWS Config 중지하면 이전에 캡처된 구성 정보가 유지되며이 정보에 계속 액세스할 수 있습니다.

레코딩을 중지하는 방법에 대한 단계는 고객 관리형 구성 레코더 중지를 참조하세요.

를 사용하여 타사 리소스 AWS Config 용를 사용하여 구성 기록 AWS CLI

온프레미스 서버, SAAS 모니터링 도구 및 버전 제어 시스템(예: GitHub)과 같은 타사 리소스 또는 사용자 지정 리소스 유형에 대한 구성을 기록합니다.

AWS Config 콘솔 AWS Config 및 APIs. AWS Config 를 사용하여 모든 리소스를 관리하고 AWS Config 규칙을 사용하는 모범 사례에 대한 규정 준수를 위해 리소스 구성을 평가할 수 있습니다. AWS Config 규칙 또는 적합성 팩을 생성하여 모범 사례, 내부 정책 및 규제 정책과 비교하여 이러한 타사 리소스를 평가할 수도 있습니다.

> **Note**
>
> 모든 리소스 유형을 기록 AWS Config 하도록를 구성한 경우를 통해 관리(생성, 업데이트 또는 삭제)되는 타사 리소스는에서 구성 항목 AWS Config 으로 자동으로 추적 AWS CloudFormation 됩니다.

사전 조건: 타사 리소스 또는 사용자 지정 리소스 유형은를 사용하여 등록해야 합니다 AWS CloudFormation.

주제

- 에 타사 리소스 추가 AWS Config
- 를 사용하여 타사 리소스 AWS Config 에 대한를 사용하여 구성 항목 기록 AWS CLI
- 를 사용하여 타사 리소스 AWS Config 용를 사용하여 구성 항목 읽기 AWS CLI
- 를 사용하여에서 AWS Config 타사 리소스 삭제 AWS CLI

에 타사 리소스 추가 AWS Config

다음 단계에 따라 AWS Config에 타사 리소스를 추가합니다.

주제

- 1단계: 개발 환경 설정
- 2단계: 리소스 모델링
- 3단계: 아티팩트 생성
- 4단계: 리소스 등록
- 5단계: 리소스 구성 게시

1단계: 개발 환경 설정

AWS CloudFormation AWS CLI를 설치하고 구성합니다. 를 AWS CLI 사용하면 사용자 지정 리소스를 모델링하고 등록할 수 있습니다. 자세한 내용은 사용자 지정 리소스 및 CloudFormation 명령줄 인터페이스란 무엇입니까?를 참조하세요.

2단계: 리소스 모델링

리소스 유형의 구성을 준수하고 검증하는 리소스 공급자 스키마를 만듭니다.

1. `init` 명령을 사용하여 리소스 공급자 프로젝트를 만들고 필요한 파일을 생성합니다.

   ```
   $ cfn init
   Initializing new project
   ```

2. 이 `init` 명령은 리소스 이름을 지정하는 등 프로젝트 설정을 안내하는 마법사를 시작합니다. 이 연습에서는 `MyCustomNamespace::Testing::WordPress`를 지정합니다.

```
Enter resource type identifier (Organization::Service::Resource):
 MyCustomNamespace::Testing::WordPress
```

3. 리소스의 패키지 이름을 입력합니다.

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

> **Note**
>
> 프로젝트 종속성이 올바르게 해결되도록 Maven 지원을 통해 생성된 프로젝트를 IDE로 가져올 수 있습니다.
> 예를 들어 IntelliJ IDEA를 사용하고 있는 경우에는 다음을 수행해야 합니다.
>
> - 파일 메뉴에서 신규를 선택한 다음, 기존 소스의 프로젝트를 선택합니다.
> - 프로젝트 디렉터리로 이동합니다.
> - 프로젝트 가져오기 대화 상자에서 외부 모델에서 프로젝트 가져오기를 선택한 다음 Maven을 선택합니다.
> - 다음을 선택하고 기본값을 모두 그대로 사용하여 프로젝트 가져오기를 완료합니다.

4. 리소스에 대한 스키마가 포함된 `mycustomnamespace-testing-wordpress.json` 파일을 엽니다. 다음 스키마를 복사하여 `mycustomnamespace-testing-wordpress.json`에 붙여 넣습니다.

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
```

```
      "type": "string"
    },
    "InstanceId": {
      "description": "The ID of the instance that backs the WordPress site.",
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. 스키마를 검증합니다.

```
$ cfn validate
```

6. 리소스 공급자 패키지에 자동 생성된 파일을 업데이트하여 리소스 공급자 스키마 업데이트를 확인합니다. 리소스 공급자 프로젝트를 시작하면는 리소스 공급자에 대한 지원 파일과 코드를 AWS CLI 생성합니다. 업데이트된 스키마를 보려면 코드를 다시 생성합니다.

```
$ cfn generate
```

> **Note**
>
> Maven을 사용하는 경우 빌드 프로세스의 일부로 코드가 컴파일되기 전에 `generate` 명령이 자동으로 실행됩니다. 따라서 변경 사항이 생성된 코드와 항상 동기화됩니다. CloudFormation CLI는 Maven/시스템이 찾을 수 있는 위치에 있어야 합니다. 자세한 내용은 익스텐션 개발을 위한 환경 설정을 참조하세요.

전체 프로세스에 대한 자세한 내용은 AWS CloudFormation에서 사용할 리소스 공급자 모델링을 참조하세요.

3단계: 아티팩트 생성

다음 명령을 실행하여 `cfn submit`에 대한 아티팩트를 생성합니다.

```
$ mvn package
```

4단계: 리소스 등록

AWS Config 에서는 리소스 공급자 핸들러가 리소스에 대한 구성 추적을 수행할 필요가 없습니다. 다음 명령을 실행하여 리소스를 등록합니다.

```
$ cfn submit
```

자세한 내용은 AWS CloudFormation 템플릿에서 사용할 리소스 공급자 등록을 참조하세요.

5단계: 리소스 구성 게시

MyCustomNamespace::Testing::WordPress에 대한 구성을 결정합니다.

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

스키마 버전 ID를 결정합니다 AWS CloudFormation `DescribeType`.

에서이 리소스 구성이 수락되었는지 확인할 AWS Config수 있습니다. 규정 준수를 평가하기 위해이 리소스를 사용하여 AWS Config 규칙을 작성할 수 있습니다.

(선택 사항) 구성 기록을 자동화하려면 주기적 또는 변경 기반 구성 수집기를 구현합니다.

를 사용하여 타사 리소스 AWS Config 에 대한를 사용하여 구성 항목 기록 AWS CLI

다음 절차에 따라 타사 리소스 또는 사용자 지정 리소스 유형에 대한 구성 항목을 기록합니다.

리소스 유형 `MyCustomNamespace::Testing::WordPress`를 일치하는 스키마에 등록해야 합니다.

1. 명령 프롬프트 또는 터미널 창을 엽니다.
2. 다음 명령을 입력합니다.

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> 형식 스키마에 정의된 대로 `writeOnlyProperties`는에서 기록되기 전에 구성에서 제거됩니다 AWS Config. 읽기 API를 통해 구성을 가져올 때는 이러한 값이 표시되지 않습니다. `writeOnlyProperties`에 대한 자세한 내용은 리소스 유형 스키마를 참조하세요.

를 사용하여 타사 리소스 AWS Config 용를 사용하여 구성 항목 읽기 AWS CLI

다음 절차에 따라 타사 리소스 또는 사용자 지정 리소스 유형에 대한 구성 항목을 읽습니다.

1. 명령 프롬프트 또는 터미널 창을 엽니다.
2. 다음 명령을 입력합니다.

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. Enter를 누릅니다.

   다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
        }
    ]
}
```

4. 다음 명령을 입력합니다.

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. Enter를 누릅니다.

   다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
        }
    ]
}
```

를 사용하여에서 AWS Config 타사 리소스 삭제 AWS CLI

타사 리소스를 삭제하려면 다음 명령을 입력합니다.

```
aws configservice delete-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

명령이 성공하면 추가 출력이 표시되지 않습니다.

를 사용하여 관리형 인스턴스에 대한 소프트웨어 구성 기록 AWS Config

AWS Config 를 사용하여 Amazon EC2 인스턴스 및 온프레미스 서버의 소프트웨어 인벤토리 변경 사항을 기록할 수 있습니다. 이를 통해 소프트웨어 구성의 변경 기록을 볼 수 있습니다. 예를 들어 관리형 Windows 인스턴스에 새 Windows 업데이트가 설치되면는 변경 사항을 AWS Config 기록한 다음 전송 채널로 변경 사항을 전송하여 변경 사항에 대한 알림을 받습니다. 를 사용하면 관리형 인스턴스에 Windows 업데이트가 설치된 시기의 기록과 시간이 지남에 따라 변경된 방식을 확인할 AWS Config수 있습니다.

주제

- 사전 조건
- 소프트웨어 구성 레코딩

사전 조건

소프트웨어 구성 변경을 기록하려면 다음 단계를 완료해야 합니다.

- AWS Config에서 관리형 인스턴스 인벤토리 리소스 유형에 대한 기록을 켭니다.
- EC2 및 온프레미스 서버를에서 관리형 인스턴스로 구성합니다 AWS Systems Manager. 관리형 인스턴스는 Systems Manager에 사용하도록 구성된 시스템입니다.
- Systems Manager 인벤토리 기능을 사용하여 관리형 인스턴스에서 소프트웨어 인벤토리 수집을 시작합니다.

> **Note**
>
> Systems Manager는 이제 비관리형 인스턴스에 대한 구성 항목 생성을 지원합니다.
> 비관리형 인스턴스의 구성 항목에는 `Key: “InstanceStatus”` 및 `Value: “Unmanaged”`가 포함된 추가 구성이 있습니다.
> 비관리형 인스턴스의 구성 항목은 추가 업데이트를 받지 않습니다.
> 추가 업데이트를 받으려면 구성 항목이 관리형 인스턴스여야 합니다.

또한 AWS Config 규칙을 사용하여 소프트웨어 구성 변경을 모니터링하고 변경 사항이 규칙을 준수하는지 또는 준수하지 않는지 여부를 알릴 수 있습니다. 예를 들어, 관리형 인스턴스에 지정된 애플리케이션이 있는지 확인하는 규칙을 만들었는데 인스턴스에 해당 애플리케이션이 설치되지 않은 경우

AWS Config 는 해당 인스턴스를 규칙 미준수로 표시합니다. AWS Config 관리형 규칙 목록은 섹션을 참조하세요AWS Config 관리형 규칙 목록.

소프트웨어 구성 레코딩

AWS Config에서 소프트웨어 구성 변경 기록을 활성화하려면

1. AWS Config가 지원하는 모든 리소스 유형에 대한 기록을 켜거나 관리형 인스턴스 인벤토리 리소스 유형을 선택적으로 기록합니다. 자세한 내용은 를 사용하여 AWS 리소스 기록 AWS Config 단원을 참조하십시오.
2. AmazonSSM ManagedInstanceCore 관리형 정책을 포함하는 Systems Manager용 인스턴스 프로파일을 사용하여 Amazon EC2 인스턴스를 시작합니다. 이 AWS 관리형 정책을 사용하면 인스턴스가 Systems Manager 서비스 핵심 기능을 사용할 수 있습니다.

   Systems Manager에 대한 인스턴스 프로파일에 추가할 수 있는 다른 정책에 대한 자세한 정보는 AWS Systems Manager 사용 설명서의 Systems Manager에 대한 IAM 인스턴스 프로파일 생성을 참조하세요.

   > **Important**
   >
   > SSM 에이전트는 클라우드에서 Systems Manager와 통신하기 위해 관리형 인스턴스에 설치해야 하는 Amazon 소프트웨어입니다. EC2 인스턴스가 다음 운영 체제 중 하나에 대해 AMI에서 생성된 경우 에이전트가 미리 설치됩니다.
   >
   > - Windows Server 2003-2012 R2 AMI는 2016년 11월 이후에 게시되었습니다.
   > - Windows Server 2016 및 2019
   > - Amazon Linux
   > - Amazon Linux 2
   > - Ubuntu Server 16.04
   > - Ubuntu Server 18.04
   >
   > 에이전트가 미리 설치된 AMI에서 생성되지 않은 EC2 인스턴스에서는 에이전트를 수동으로 설치해야 합니다. 자세한 내용은 AWS Systems Manager 사용 설명서에서 다음 주제를 참조하세요.
   >
   > - Windows Server용 EC2 인스턴스에 SSM 에이전트 설치 및 구성

- Linux용 EC2 인스턴스에 SSM 에이전트 설치 및 구성

3. AWS Systems Manager 사용 설명서의 인벤토리 수집 구성에 설명된 대로 인벤토리 수집을 시작합니다. Linux 인스턴스나 Windows 인스턴스나 절차는 동일합니다.

   AWS Config 는 다음 인벤토리 유형에 대한 구성 변경을 기록할 수 있습니다.

   - 애플리케이션 - 관리형 인스턴스의 애플리케이션 목록입니다(예: 안티바이러스 소프트웨어).
   - AWS 구성 요소 - AWS CLI 및 SDK와 같은 관리형 인스턴스의 구성 요소 목록 AWS 입니다. SDKs
   - 인스턴스 정보 - 인스턴스 정보입니다(예: OS 이름 및 버전, 도메인, 방화벽 상태).
   - 네트워크 구성 - 구성 정보입니다(예: IP 주소, 게이트웨이, 서브넷 마스크).
   - Windows 업데이트 - 관리형 인스턴스의 Windows 업데이트 목록입니다(Windows 인스턴스만 해당).

   > **Note**
   >
   > AWS Config 는 현재 사용자 지정 인벤토리 유형 기록을 지원하지 않습니다.

인벤토리 수집은 많은 Systems Manager 기능 중의 하나며 작업 관리, 작업 및 변경, 인스턴스 및 노드 그리고 공유 리소스 카테고리에서 그룹화됩니다. 자세한 내용은 Systems Manager란 무엇인가요? 및 AWS Systems Manager 사용 설명서의의 Systems Manager 기능을 참조하세요.

에서 검색한 리소스 조회 AWS Config

AWS Config 콘솔 AWS CLI및 AWS Config API를 사용하여 삭제 AWS Config 된 리소스 및 현재 기록되지 않은 리소스를 포함하여 인벤토리를 가져오거나 검색한 리소스를 조회할 수 있습니다. AWS Config 는 지원되는 리소스 유형만 AWS Config 검색합니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.

Looking Up Resources (Console)

AWS Config 콘솔에서 리소스 유형 또는 태그 정보를 사용해 리소스를 조회할 수 있습니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.

2. 리소스 인벤토리 페이지에서 조회할 리소스의 검색 옵션을 다음을 참조하여 지정합니다.
   - 리소스 범주 - 모든 리소스 범주를 선택하거나 결과를 AWS 리소스로만 좁힙니다.
   - 리소스 유형 - 모든 리소스 유형을 선택하거나 필터링 기준으로 사용할 리소스를 선택합니다.
   - 규정 준수 - 규정 준수 상태, 규정 준수 또는 비준수 기준으로 필터링하도록 선택합니다.
3. AWS Config 는 검색 옵션과 일치하는 리소스를 나열합니다. 리소스에 대한 다음 정보를 확인할 수 있습니다.
   - 리소스 식별자는 리소스 ID 또는 리소스 이름(해당되는 경우)일 수 있습니다. 리소스 식별자 링크를 선택하여 리소스의 세부 정보 페이지를 볼 수 있습니다.
   - 리소스 유형 - 표시된 리소스의 유형
   - 규정 준수 - 규칙에 대해 AWS Config 평가된 리소스의 상태입니다.

Looking Up Resources (AWS CLI)

를 사용하여에서 검색한 리소스를 나열 AWS CLI 할 수 AWS Config 있습니다.

AWS Config service **`list-discovered-resources`** 명령을 사용합니다.

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
            "resourceIdentifiers": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-nnnnnnnn"
                }
            ]
        }
```

반환된 목록에 표시된 리소스의 구성 세부 정보를 확인하려면 `get-resource-config-history` 명령을 사용하고 리소스 유형 및 ID를 지정합니다. 이 명령의 예제와의 응답은 단원을 AWS Config 참조하십시오구성 기록 보기.

Looking up Resources (API)

리소스 유형을 지정하면 해당 유형의 리소스에 대한 리소스 식별자 목록이 AWS Config 반환됩니다. 자세한 내용은 AWS Config API 참조의 ResourceIdentifier를 참조하세요.

ListiscoveredResources 작업을 사용합니다.

응답에 나열된 리소스의 구성 세부 정보를 확인하려면 GetResourceConfigHistory 작업을 사용하고 리소스 유형 및 ID를 지정합니다.

를 사용하여 AWS 리소스에 대한 규정 준수 정보 및 평가 결과 보기 AWS Config

> **Important**
>
> 규정 준수 상태를 정확하게 보고하려면 `AWS::Config::ResourceCompliance` 리소스 유형을 반드시 기록해야 합니다. 자세한 내용은 AWS 리소스 기록을 참조하세요.

AWS Config 콘솔 또는 AWS SDKs를 사용하여 규정 준수 정보와 리소스의 평가 결과를 볼 수 있습니다.

주제

- 규정 준수 상태 보기(콘솔)
- 규정 준수(AWS SDKs) 보기

규정 준수 상태 보기(콘솔)

규정 준수 상태 확인(콘솔)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Management Console 메뉴에서 리전 선택기가 AWS Config 규칙을 지원하는 리전으로 설정되어 있는지 확인합니다. 지원되는 리전의 목록은 Amazon Web Services 일반 참조의 AWS Config 리전 및 엔드포인트를 참조하세요.
3. 탐색 창에서 Resources를 선택합니다. 리소스 인벤토리 페이지에서 리소스 범주, 리소스 유형 및 규정 준수 상태를 기준으로 필터링할 수 있습니다. 필요한 경우 삭제된 리소스 포함을 선택합니다. 이 표에는 리소스 유형의 리소스 식별자와 해당 리소스에 대한 리소스 준수 상태가 표시됩니다. 리소스 식별자는 리소스 ID 또는 리소스 이름일 수 있습니다.
4. 리소스 식별자 열에서 리소스를 선택합니다.
5. 리소스 타임라인 버튼을 선택합니다. 구성 이벤트, 규정 준수 이벤트 또는 CloudTrail 이벤트를 기준으로 필터링할 수 있습니다.

> **Note**
> 또는 리소스 인벤토리 페이지에서 리소스 이름을 직접 선택합니다. 리소스 세부 정보 페이지에서 리소스 타임라인에 액세스하려면 리소스 타임라인 버튼을 선택합니다.

리소스 인벤토리 페이지에서 리소스를 찾아 리소스의 준수 상태를 볼 수도 있습니다. 자세한 내용은 에서 검색한 리소스 조회 AWS Config 단원을 참조하십시오.

규정 준수(AWS SDKs) 보기

AWS 리소스에 대한 규정 준수 정보를 가져오는 방법

다음 코드 예시는 `DescribeComplianceByResource`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS 리소스에 대한 규정 준수 정보를 가져오는 방법

다음 명령은 AWS Config에 의해 기록되고 하나 이상의 규칙을 위반하는 각 EC2 인스턴스에 대한 규정 준수 정보를 반환합니다.

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

출력에서 각 `CappedCount` 속성의 값은 리소스가 위반한 규칙의 수를 나타냅니다. 예를 들어 다음 출력은 인스턴스 `i-1a2b3c4d`가 2개의 규칙을 위반함을 나타냅니다.

출력:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
```

```
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeComplianceByResource 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제에서는 **`AWS::SSM::ManagedInstanceInventory`** 리소스 유형에 'COMPLIANT' 규정 준수 유형이 있는지 확인합니다.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

출력:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- API 세부 정보는 Cmdlet 참조(V4)의 DescribeComplianceByResource를 참조하세요. AWS Tools for PowerShell

AWS 리소스의 규정 준수 요약을 가져오는 방법

다음 코드 예시는 `GetComplianceSummaryByResourceType`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

모든 리소스 유형에 대한 규정 준수 요약을 가져오려면

다음 명령은 규정을 준수하지 않는 AWS 리소스 수와 규정을 준수하는 리소스 수를 반환합니다.

```
aws configservice get-compliance-summary-by-resource-type
```

출력에서 각 `CappedCount` 속성의 값은 규정 준수 또는 규정 미준수 리소스 수를 나타냅니다.

출력:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

특정 리소스 유형에 대한 규정 준수 요약을 가져오는 방법

다음 명령은 규정을 준수하지 않는 EC2 인스턴스 수와 규정을 준수하는 EC2 인스턴스 수를 반환합니다.

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

출력에서 각 CappedCount 속성의 값은 규정 준수 또는 규정 미준수 리소스 수를 나타냅니다.

출력:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 GetComplianceSummaryByResourceType 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 샘플은 규정 준수 또는 규정 미준수 리소스 수를 반환하고 출력을 json으로 변환합니다.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
```

```
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- API 세부 정보는 Cmdlet 참조(V4)의 GetComplianceSummaryByResourceType을 참조하세요. AWS Tools for PowerShell

AWS 리소스에 대한 평가 결과를 가져오는 방법

다음 코드 예시는 `GetComplianceDetailsByResource`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS 리소스에 대한 평가 결과를 가져오는 방법

다음 명령은 EC2 인스턴스 `i-1a2b3c4d`가 준수하지 않는 각 규칙에 대한 평가 결과를 반환합니다.

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

출력:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
```

```
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 GetComplianceDetailsByResource 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 제공된 리소스에 대한 예제 평가 결과입니다.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

출력:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- API 세부 정보는 Cmdlet 참조(V4)의 GetComplianceDetailsByResource를 참조하세요. AWS Tools for PowerShell

를 사용하여 AWS 리소스에 대한 규정 준수 기록 보기 AWS Config

> **Important**
>
> 규정 준수 상태를 정확하게 보고하려면 `AWS::Config::ResourceCompliance` 리소스 유형을 반드시 기록해야 합니다. 자세한 내용은 AWS 리소스 기록을 참조하세요.

AWS Config 콘솔에서 리소스에 대한 구성, 관계 및 변경 횟수를 볼 수 있습니다. 를 사용하여 리소스의 구성 기록을 볼 수 있습니다 AWS CLI.

주제

- 규정 준수 이력 보기(콘솔)
- 규정 준수 이력 보기(AWS CLI)
- 리소스 및 규칙 규정 준수 기록 타임라인 보기

규정 준수 이력 보기(콘솔)

콘솔을 사용하여 규정 준수 기록 보기

리소스 인벤토리 페이지에서 리소스를 조회할 때 리소스 식별자 열에서 리소스 이름 또는 ID를 선택하여 리소스 세부 정보 페이지를 볼 수 있습니다. 세부 정보 페이지에서는 구성, 관계, 리소스 변경 사항 수에 대한 정보를 확인할 수 있습니다.

리소스 세부 정보 페이지에서 리소스 타임라인에 액세스하려면 리소스 타임라인 버튼을 선택합니다. 리소스 타임라인은 특정 리소스에 대해 일정 시간의 기간 동안 변경 사항을 `ConfigurationItems`로 캡처합니다. 구성 이벤트, 규정 준수 이벤트 또는 CloudTrail 이벤트를 기준으로 필터링할 수 있습니다.

규정 준수 이력 보기(AWS CLI)

를 사용하여 규정 준수 기록 보기 AWS CLI

에서 AWS Config 기록하는 구성 항목은 지정된 전송 채널에 구성 스냅샷 및 구성 스트림으로 온디맨드로 전달됩니다. AWS CLI 를 사용하여 각 리소스의 구성 항목 기록을 볼 수 있습니다.

구성 기록 보기

예를 들어 다음과 같이 `get-resource-config-history` 명령을 입력하고 리소스 유형과 리소스 ID를 지정합니다.

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
```

```
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```

응답 필드에 대한 자세한 설명은 Components of a Configuration Item 및 에 대해 지원되는 리소스 유형 AWS Config 문서를 참조하세요.

AWS Config의 Amazon EBS 구성 기록 예

AWS Config 는 각각 리소스 유형을 나타내는 파일 세트를 생성하고 기록 중인 해당 유형의 리소스에 대한 모든 구성 변경 사항을 나열합니다. AWS Config AWS Config 는이 리소스 중심 구성 기록을 활성화할 때 지정한 Amazon S3 버킷의 객체로 내보냅니다 AWS Config. 각 리소스 유형의 구성 기록 파일에는 마지막 기록 파일이 전달된 이후 해당 유형의 리소스에 대해 발견된 변경 사항이 포함됩니다. 기록 파일은 일반적으로 6시간마다 전달됩니다.

다음은 AWS 계정의 현재 리전에 있는 모든 Amazon Elastic Block Store 볼륨의 구성 기록을 설명하는 Amazon S3 객체의 콘텐츠 예입니다. 이 계정의 볼륨에는 `vol-ce676ccc` 및 `vol-cia007c`가 포함되어 있습니다. 볼륨 `vol-ce676ccc`에는 이전 기록 파일이 전달된 이후로 두 개의 구성 변경이 있었던 반면, 볼륨 `vol-cia007c`에는 하나의 구성 변경이 있습니다.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
```

```
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
```

```
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-ad229edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04w292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
```

```
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-cia007c",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a67u292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T20:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344e563d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-cia007c",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
```

```
                        "volumeId": "vol-cia007c",
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

리소스 및 규칙 규정 준수 기록 타임라인 보기

AWS Config 는에서 평가한 리소스의 규정 준수 상태 변경 사항 저장을 지원합니다 AWS Config 규칙. 리소스 규정 준수 이력은 타임라인 형식으로 표시됩니다. 타임라인은 특정 리소스에 대해 일정 시간의 기간 동안 변경 사항을 `ConfigurationItems`로 캡처합니다. 의 내용에 대한 자세한 `ConfigurationItem`내용은 AWS Config API 참조의 ConfigurationItem을 참조하세요.

AWS Config의 모든 리소스 유형을 기록하도록 수락 또는 거부할 수 있습니다. 모든 리소스 유형을 기록하도록 선택한 경우는 평가된 대로 리소스 규정 준수 기록 기록을 AWS Config 자동으로 시작합니다 AWS Config 규칙. 기본적으로는 지원되는 모든 리소스에 대한 구성 변경 사항을 AWS Config 기록합니다. `AWS::Config::ResourceCompliance`를 통해 특정 리소스 규정 준수 이력 유형만 선택할 수도 있습니다. 자세한 내용은 AWS 레코드 기록을 참조하세요.

Viewing Resource Timeline Using Resources

리소스 인벤토리 페이지에서 특정 리소스를 선택하여 리소스 타임라인을 볼 수 있습니다.

1. 왼쪽 탐색 창에서 리소스를 선택합니다.

2. 리소스 인벤토리 페이지에서 리소스 범주, 리소스 유형, 규정 준수 상태별로 필터링할 수 있습니다. 필요한 경우 삭제된 리소스 포함을 선택합니다.

   이 표에는 리소스 유형의 리소스 식별자와 해당 리소스에 대한 리소스 준수 상태가 표시됩니다. 리소스 식별자는 리소스 ID 또는 리소스 이름일 수 있습니다.
3. 리소스 식별자 열에서 리소스를 선택합니다.
4. 리소스 타임라인 버튼을 선택합니다. 구성 이벤트, 규정 준수 이벤트 또는 CloudTrail 이벤트를 기준으로 필터링할 수 있습니다.

> **Note**
>
> 또는 리소스 인벤토리 페이지에서 리소스 이름을 직접 선택합니다. 리소스 세부 정보 페이지에서 리소스 타임라인에 액세스하려면 리소스 타임라인 버튼을 선택합니다.

Viewing Resource Timeline Using Rules

규칙 페이지에서 특정 규칙을 선택하여 리소스 타임라인을 볼 수 있습니다.

1. 왼쪽 탐색 창에서 규칙을 선택합니다.
2. 규칙 페이지에서 해당 리소스를 평가하는 규칙을 선택합니다. 화면에 규칙이 표시되지 않을 경우 규칙 추가 버튼을 사용하여 규칙을 추가합니다.
3. 규칙 세부 정보 페이지의 리소스 평가 테이블에서 리소스를 선택합니다.
4. 리소스 타임라인 버튼을 선택합니다. 리소스 타임라인이 표시됩니다.

AWS 리소스에 대한 규정 준수 기록 쿼리

`AWS::Config::ResourceCompliance` 리소스 유형을 사용하여 get-resource-config-history를 통해 리소스 규정 준수 이력을 쿼리합니다.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
 "configurationItems": [
  {
```

```
    "configurationItemCaptureTime": 1539799966.921,
    "relationships": [
     {
      "resourceType": "AWS::S3::Bucket",
      "resourceId": "configrules-bucket",
      "relationshipName": "Is associated with "
     }
    ]
    "tags": {},
    "resourceType": "AWS::Config::ResourceCompliance",
    "resourceId": "AWS::S3::Bucket/configrules-bucket",
    "ConfigurationStateId": "1539799966921",
    "relatedEvents": [];
    "awsRegion": "us-west-2",
    "version": "1.3",
    "configurationItemMD5Hash": "",
    "supplementaryConfiguration": {},
    "configuration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":
\"configrules-bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList"\":
[{\"configRuleArn\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw
\",\"configRuleId\":\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-
enabled\",\"complianceType\":\"COMPLIANT\"}]}",

    "configurationItemStatus": "ResourceDiscovered",
    "accountId": "AccountID"
   }
  ]
}
```

AWS Config 리소스 태그 지정

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 사용자가 정의하는 키와 선택적 값으로 구성됩니다. 태그를 사용하면 리소스를 보다 쉽게 관리, 검색 및 필터링할 수 있습니다.

태그를 사용하면 용도, 소유자 또는 환경 등 다양한 방식으로 AWS 리소스를 분류할 수 있습니다. 이 기능은 지정한 태그에 따라 특정 리소스를 빠르게 식별할 수 있으므로 동일한 유형의 리소스가 많을 때 유용합니다. AWS 리소스에 하나 이상의 태그를 할당할 수 있습니다. 각 태그에는 연결된 값이 있습니다.

각 리소스 유형에 대한 요건을 충족하는 태그 키 세트를 고안하는 것이 좋습니다. 일관된 태그 키 세트를 사용하면 AWS 리소스를 보다 쉽게 관리할 수 있습니다. 추가하는 태그에 따라 리소스를 검색하고 필터링할 수 있습니다.

태그는 엄격히 문자열로 해석되며 리소스에 자동으로 할당되지 않습니다. 태그 키와 값을 편집할 수 있으며 언제든지 리소스에서 태그를 제거할 수 있습니다. 태그의 값을 빈 문자열로 설정할 수 있지만 태그의 값을 Null로 설정할 수는 없습니다. 해당 리소스에 대해 키가 기존 태그와 동일한 태그를 추가하는 경우 새 값이 이전 값을 덮어씁니다. 리소스를 삭제하면 리소스 태그도 삭제됩니다.

AWS Command Line Interface (AWS CLI) 및 AWS Config API 참조를 사용하여 태그로 작업할 수 있습니다.

태그 지정에 관련된 제한

태그에 적용되는 기본 제한은 다음과 같습니다.

제한	설명
리소스당 최대 태그 수	50
최대 키 길이	UTF-8 형식의 유니코드 문자 128자
최대 값 길이	UTF-8 형식의 유니코드 문자 256자
접두사 제한	태그 이름 또는 값은 AWS 사용하기 위해 예약되어 있으므로 `aws:` 접두사를 사용하지 마세요. 이 접두사가 지정된 태그 이름이나 값은 편집하거나 삭제할 수 없습니다. 이 접두사가 지정된 태그는 리소스당 태그 수 제한에 포함되지 않습니다.
문자 제한	태그에는 유니코드 문자, 숫자, 공백 또는 `_ . : / = + - @` 등의 기호만 사용할 수 있습니다.

AWS Config API 작업을 사용한 태그 관리

`ConfigurationAggregator`, `AggregationAuthorization` 및 `ConfigRule` 리소스에 대해 태그 기반 액세스 제어를 사용할 수 있습니다. 다음을 사용하여 리소스에 대한 태그를 추가, 업데이트, 나열 및 삭제할 수 있습니다.

- ListTagsForResource

- TagResource
- UntagResource

> **Note**
>
> `TagResource` 및는 액세스를 제어하려면 특정 AWS Identity and Access Management (IAM) 권한이 `UntagResource` 필요합니다. 자세한 내용은 IAM 사용 설명서의 태그 키를 기반으로 액세스 제어를 참조하세요.

AWS Config 규칙을 사용하여 리소스 평가

AWS Config 를 사용하여 AWS 리소스의 구성 설정을 평가합니다. 이를 위해 이상적인 구성 설정을 나타내는 AWS Config 규칙을 생성합니다.는 시작하는 데 도움이 되는 관리형 규칙이라고 하는 사용자 지정 가능한 사전 정의된 규칙을 AWS Config 제공합니다.

주제

- 고려 사항
- 리전 지원
- AWS Config 규칙의 구성 요소
- AWS Config 관리형 규칙
- AWS Config 사용자 지정 규칙
- 서비스 연결 AWS Config 규칙
- 조직의 모든 계정에서 AWS Config 규칙 관리
- AWS Config 규칙 추가
- AWS Config 규칙 업데이트
- AWS Config 규칙 삭제
- AWS Config 규칙에 대한 세부 정보 및 규정 준수 정보 보기
- AWS Config 규칙에 대한 사전 평가 켜기
- 규칙 평가를 Security Hub로 전송
- AWS Config 규칙을 사용하여 리소스 평가
- AWS Config 규칙에서 평가 결과 삭제
- AWS Config 규칙 문제 해결

고려 사항

Cost Considerations

리소스 기록과 관련된 비용에 대한 자세한 내용은 AWS Config 요금을 참조하세요.

권장 사항: 규칙을 삭제하기 전에 **`AWS::Config::ResourceCompliance`** 리소스 유형을 기록에서 제외하는 것이 좋습니다.

규칙을 삭제하면 구성 레코더 비용에 영향을 미칠 수 `AWS::Config::ResourceCompliance` 있는에 대한 구성 항목(CIs)이 생성됩니다. 많은 수의 리소스 유형을 평가하는 규칙을 삭제하는 경우 기록된 CI의 수가 급증할 수 있습니다.

관련 비용을 방지하려면 규칙을 삭제하기 전에 `AWS::Config::ResourceCompliance` 리소스 유형에 대한 기록을 비활성화하고 규칙이 삭제된 후 기록을 다시 활성화하도록 선택할 수 있습니다.

그러나 규칙 삭제는 비동기 프로세스이므로 완료하는 데 1시간 이상 걸릴 수 있습니다. 에 대한 레코딩이 비활성화된 시간 동안에는 `AWS::Config::ResourceCompliance`규칙 평가가 연결된 리소스의 기록에 기록되지 않습니다.

AWS Config 에서는 규칙 삭제를 진행하기 전에 이러한 요소를 case-by-case 평가할 것을 권장합니다.

권장 사항: 사용자 지정 lambda 규칙에 대해 삭제된 리소스 평가를 처리하는 로직 추가

AWS Config 사용자 지정 Lambda 규칙을 생성할 때는 삭제된 리소스의 평가를 처리하는 로직을 추가하는 것이 좋습니다.

평가 결과가 `NOT_APPLICABLE`로 표시되면 해당 리소스가 삭제로 표시되고 정리됩니다. `NOT_APPLICABLE`로 표시되지 않을 경우 규칙이 삭제될 때까지 평가 결과는 변경되지 않으며, 이로 인해 규칙 삭제 시 `AWS::Config::ResourceCompliance`에 대한 구성 항목(CI) 생성이 예기치 않게 급증할 수 있습니다.

삭제된 리소스에 대해 반환하도록 AWS Config 사용자 지정 Lambda 규칙을 설정하는 방법에 `NOT_APPLICABLE` 대한 자세한 내용은 사용자 AWS Config 지정 Lambda 규칙을 사용하여 삭제된 리소스 관리를 참조하세요.

권장 사항: 사용자 지정 lambda 규칙의 범위 내 리소스 제공

AWS Config 규칙의 범위가 하나 이상의 리소스 유형으로 지정되지 않은 경우 사용자 지정 Lambda 규칙으로 인해 Lambda 함수 호출이 많이 발생할 수 있습니다. 계정과 관련된 활동이 증가하지 않도록 사용자 지정 Lambda 규칙 범위에 속하는 리소스를 제공하는 것이 권장됩니다. 리소스 유형을 선택하지 않은 경우 규칙은 계정의 모든 리소스에 대해 Lambda 함수를 간접 호출합니다.

Other considerations

관리형 규칙의 기본값

관리형 규칙에 지정된 기본값은 AWS 콘솔을 사용할 때만 미리 채워집니다. API, CLI 또는 SDK에는 기본값이 제공되지 않습니다.

구성 항목 레코딩 지연

AWS Config 는 일반적으로 변경 사항이 감지된 직후 또는 지정한 빈도로 리소스에 대한 구성 변경 사항을 기록합니다. 그러나 이는 가장 이상적인 시나리오이며 경우에 따라 더 오래 걸릴 수 있습니다. 예를 들어 지연이 알려진 리소스 유형은 입니다`AWS::SecretsManager::Secret`. 이 리소스 유형은 예제이며이 목록은 포괄적이지 않습니다.

정책 및 규정 준수 결과

에서 관리되는 IAM 정책 및 기타 정책은 AWS Config 에 리소스에 대한 구성 변경을 기록할 권한이 있는지 여부에 영향을 미칠 수 있습니다. AWS Organizations 또한 규칙은 리소스의 구성을 직접 평가하며, 규칙은 평가를 실행할 때 이러한 정책을 고려하지 않습니다. 적용 중인 정책이 사용 의도와 일치하는지 확인합니다 AWS Config.

리소스 유형에 대한 태그 지정 지원

리소스 유형이 태그 지정을 지원하지 않거나 API 응답 설명에 태그 정보를 포함하지 않는 경우 AWS Config 는 해당 리소스 유형의 구성 항목(CIs)에 태그 데이터를 캡처하지 않습니다. AWS Config 는 여전히 이러한 리소스를 기록합니다. 그러나 태그 데이터에 의존하는 기능은 작동하지 않습니다. 이는 태그 데이터에 의존하는 태그 기반 필터링, 그룹화 또는 규정 준수 평가에 영향을 미칩니다.

디렉터리 버킷이 지원되지 않음

관리형 규칙은 Amazon Simple Storage Service(Amazon S3) 리소스를 평가할 때 범용 버킷만 지원합니다. 범용 버킷과 디렉터리 버킷에 대한 자세한 내용은 Amazon S3 사용 설명서의 버킷 개요 및 디렉터리 버킷을 참조하세요.

관리형 규칙 및 글로벌 IAM 리소스 유형

2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사용 가능한 AWS 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 리소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에서는 기록할 수 없습니다. 해당 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.

주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.

불필요한 평가를 방지하려면 지원되는 리전 중 하나에만 글로벌 IAM 리소스 유형에 대해 규정 준수를 보고하는 주기적 규칙을 배포해야 합니다. 리전에서 지원되는 관리형 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.

리전 지원

현재 AWS Config 규칙 기능은 다음 AWS 리전에서 지원됩니다. 리전에서 지원되는 개별 AWS Config 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.

리전 이름	지역	엔드포인트	프로토콜
미국 동부(오하이오)	us-east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS
미국 동부(버지니아 북부)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
미국 서부(캘리포니아 북부)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
미국 서부(오레곤)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
아프리카(케이프타운)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
아시아 태평양(홍콩)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
아시아 태평양(하이데라바드)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(자카르타)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
아시아 태평양(말레이시아)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
아시아 태평양(멜버른)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
아시아 태평양(뭄바이)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
아시아 태평양(오사카)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
아시아 태평양(서울)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
아시아 태평양(시드니)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
아시아 태평양(타이베이)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(태국)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
아시아 태평양(도쿄)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
캐나다(중부)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
캐나다 서부(캘거리)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
유럽(프랑크푸르트)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
유럽(아일랜드)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
유럽(런던)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
유럽(밀라노)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
유럽(파리)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
유럽(스페인)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
유럽(스톡홀름)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
유럽(취리히)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
이스라엘(텔아비브)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
멕시코(중부)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
중동(바레인)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
중동(UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
남아메리카(상파울루)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 동부)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 서부)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS 조직의 멤버 계정에 AWS Config 규칙 배포는 다음 리전에서 지원됩니다.

리전 이름	지역	엔드포인트	프로토콜
미국 동부(오하이오)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
미국 동부(버지니아 북부)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
미국 서부(캘리포니아 북부)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
미국 서부(오레곤)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
아프리카(케이프타운)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
아시아 태평양(홍콩)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
아시아 태평양(하이데라바드)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
아시아 태평양(자카르타)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
아시아 태평양(멜버른)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(뭄바이)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
아시아 태평양(오사카)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
아시아 태평양(서울)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
아시아 태평양(시드니)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
아시아 태평양(도쿄)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
캐나다(중부)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
캐나다 서부(캘거리)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
유럽(프랑크푸르트)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
유럽(아일랜드)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
유럽(런던)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
유럽(밀라노)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
유럽(파리)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
유럽(스페인)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
유럽(스톡홀름)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
유럽(취리히)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
이스라엘(텔아비브)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
중동(바레인)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
중동(UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
남아메리카(상파울루)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 동부)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜	
AWS GovCloud(미국 서부)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS	

AWS Config 규칙의 구성 요소

AWS Config 규칙은 AWS 리소스의 구성 설정을 평가합니다. 이 페이지에서는 규칙의 구성 요소에 대해 설명합니다.

주제

- AWS Config 규칙 작동 방식
- 트리거 유형
- 평가 모드
- AWS Config 규칙 메타데이터

AWS Config 규칙 작동 방식

AWS Config 는 리소스에 발생하는 구성 변경을 계속 추적하면서 이러한 변경 사항이 규칙의 조건을 위반하는지 여부를 확인합니다. 리소스가 규칙을 준수하지 않는 경우는 리소스와 규칙을 규정 미준수로 AWS Config 표시합니다.

AWS Config 규칙에 대해 네 가지 평가 결과가 있을 수 있습니다.

평가 결과	설명
`COMPLIANT`	규칙은 규정 준수 검사 조건을 통과합니다.
`NON_COMPLIANT`	규칙이 규정 준수 검사 조건에 실패합니다.
`ERROR`	필수/선택 사항 파라미터 중 하나가 유효하지 않거나 올바른 유형이 아니거나 형식이 잘못되었습니다.

평가 결과	설명
NOT_APPLICABLE	규칙의 로직을 적용할 수 없는 리소스를 필터링하는 데 사용됩니다. 예를 들어 alb-desync-mode-check 규칙은 Application Load Balancer만 검사하고 Network Load Balancer 및 Gateway Load Balancer는 무시합니다.

예를 들어 EC2 볼륨이 생성되면는 볼륨을 암호화해야 하는 규칙을 기준으로 볼륨을 평가할 수 AWS Config 있습니다. 볼륨이 암호화되지 않은 경우는 볼륨과 규칙을 규정 미준수로 AWS Config 표시합니다. AWS Config 는 모든 리소스에서 계정 전체 요구 사항을 확인할 수도 있습니다. 예를 들어, 계정의 EC2 볼륨 수가 원하는 합계 내에 유지되는지 또는 계정이 로깅에를 사용하는지 AWS Config 확인할 AWS CloudTrail 수 있습니다.

트리거 유형

계정에 규칙을 추가한 후는 리소스를 규칙의 조건과 AWS Config 비교합니다. 이 초기 평가 후는 평가가 트리거될 때마다 AWS Config 평가를 계속 실행합니다. 평가 트리거는 규칙의 일부로 정의되어 있으며, 다음 유형을 포함할 수 있습니다.

트리거 유형	설명
구성 변경	AWS Config 는 규칙의 범위와 일치하는 리소스가 있고 리소스 구성이 변경된 경우 규칙에 대한 평가를 실행합니다. 가 구성 항목 변경 알림을 AWS Config 전송한 후 평가가 실행됩니다. 규칙의 범위를 정의하여 평가를 유발하는 리소스를 선택합니다. 범위에는 다음이 포함될 수 있습니다. • 하나 이상의 리소스 유형 • 리소스 유형과 리소스 ID의 조합 • 태그 키와 값의 조합 • 기록된 모든 리소스가 생성, 업데이트 또는 삭제된 때

트리거 유형	설명
	AWS Config 는 규칙의 범위와 일치하는 리소스에 대한 변경을 감지하면 평가를 실행합니다. 범위를 사용하여 평가를 시작하는 리소스를 제한할 수 있습니다.
주기적	AWS Config 는 예를 들어 24시간마다 선택한 빈도로 규칙에 대한 평가를 실행합니다.
하이브리드	일부 규칙에는 구성 변경과 주기적 트리거가 모두 있습니다. 이러한 규칙의 경우는 구성 변경을 감지할 때와 사용자가 지정한 빈도로 리소스를 AWS Config 평가합니다.

평가 모드

AWS Config 규칙에 대한 두 가지 평가 모드가 있습니다.

평가 모드	설명
사전	리소스를 배포하기 전에 평가하려면 사전 평가를 사용합니다. 이를 통해 리소스 속성 세트를 사용하여 리소스를 정의하는 경우 해당 리전의 계정에 있는 사전 예방 규칙 세트를 고려하여 AWS 리소스 속성 세트가 COMPLIANT인지 NON_COMPLIANT인지 평가할 수 있습니다.
탐지	탐지 평가를 통해 이미 배포된 리소스를 평가합니다. 이를 통해 기존 리소스의 구성 설정을 평가할 수 있습니다.

> **Note**
>
> 사전 예방 규칙은 NON_COMPLIANT로 플래그가 지정된 리소스를 수정하거나 배포를 금지하지 않습니다.

자세한 내용은 AWS Config 규칙에 대한 사전 평가 켜기를 참조하세요.

사전 평가가 포함된 관리형 규칙 목록

사전 평가를 지원하는 관리형 규칙 목록은 평가 모드별 AWS Config 관리형 규칙 목록을 참조하세요.

사전 평가가 지원되는 리소스 유형 목록

다음은 사전 평가가 지원되는 리소스 유형의 목록입니다.

- `AWS::ApiGateway::Stage`
- `AWS::AutoScaling::AutoScalingGroup`
- `AWS::EC2::EIP`
- `AWS::EC2::Instance`
- `AWS::EC2::Subnet`
- `AWS::Elasticsearch::Domain`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::Redshift::Cluster`
- `AWS::S3::Bucket`
- `AWS::SNS::Topic`

AWS Config 규칙 메타데이터

AWS Config 규칙에는 다음과 같은 변경 가능한 메타데이터가 포함될 수 있습니다.

defaultName

defaultName은 규칙의 인스턴스에 기본적으로 지정되는 이름입니다.

description

규칙 설명은 규칙이 평가하는 내용에 대한 컨텍스트를 제공합니다. AWS Config 콘솔에서 최대 길이는 256자입니다. 모범 사례로, 규칙 설명은 ‘Checks if’로 시작하고 규정 미준수 시나리오에 대한 설명을 포함하는 것이 좋습니다. 서비스 이름은 규칙 설명에 처음 언급될 때 AWS 또는 Amazon으로 시작하여 완전히 작성해야 합니다. 예를 들어 처음 사용할 경우 CloudTrail 또는 CloudWatch 대

신 AWS CloudTrail Amazon CloudWatch를 사용할 수 있습니다. Amazon CloudWatch 이후의 참조에서는 서비스 이름을 축약하여 사용할 수 있습니다.

scope

범위는 규칙이 대상으로 하는 리소스 유형을 결정합니다. 지원되는 리소스 유형 목록은 지원되는 리소스 유형을 참조하세요.

compulsoryInputParameterDetails

compulsoryInputParameterDetails는 규칙이 평가를 수행하기 위한 필수 파라미터에 사용됩니다. 예를 들어, `access-keys-rotated` 관리형 규칙에는 `maxAccessKeyAge`가 필수 파라미터로 포함됩니다. 파라미터가 필요한 경우 (선택 사항)으로 표시되지 않습니다. 각 파라미터에 형식을 지정해야 합니다. 형식은 '문자열', 'int', 'double', 'CSV', '부울', 'StringMap'.중 하나일 수 있습니다.

optionalInputParameterDetails

optionalInputParameterDetails는 규칙이 평가를 수행하기 위한 선택적 파라미터에 사용됩니다. 예를 들어, `elasticsearch-logs-to-cloudwatch` 관리형 규칙에는 `logTypes`가 선택적 파라미터로 포함됩니다. 각 파라미터에 형식을 지정해야 합니다. 형식은 '문자열', 'int', 'double', 'CSV', '부울', 'StringMap'.중 하나일 수 있습니다.

supportedEvaluationModes

supportedEvaluationModes는 리소스 평가 시기를 결정합니다(리소스 배포 전 또는 리소스 배포 후).

`DETECTIVE`는 이미 배포된 리소스를 평가하는 데 사용됩니다. 이를 통해 기존 리소스의 구성 설정을 평가할 수 있습니다. `PROACTIVE`는 리소스를 배포하기 전에 리소스를 평가하는 데 사용됩니다.

이를 통해 리소스 속성 세트를 사용하여 리소스를 정의하는 경우 해당 리전의 계정에 있는 사전 예방 규칙 세트를 고려하여 AWS 리소스 속성 세트가 COMPLIANT인지 NON_COMPLIANT인지 평가할 수 있습니다.

supportedEvaluationModes를 `DETECTIVE`, `PROACTIVE` 또는 `DETECTIVE` 및 `PROACTIVE` 모두로 지정할 수 있습니다. 평가 모드를 지정해야 하며 이 필드는 비워둘 수 없습니다.

> **Note**
>
> 사전 예방 규칙은 NON_COMPLIANT로 플래그가 지정된 리소스를 수정하거나 배포를 금지하지 않습니다.

AWS Config 관리형 규칙

AWS Config 는가 AWS 리소스가 일반적인 모범 사례를 준수하는지 여부를 평가하는 데 AWS Config 사용하는 사전 정의되고 사용자 지정 가능한 규칙인 AWS 관리형 규칙을 제공합니다. 관리형 규칙을 사용하면 예를 들어 Amazon Elastic Block Store(Amazon EBS) 볼륨이 암호화되었는지 여부 또는 리소스에 특정 태그가 적용되어 있는지 여부 등을 신속하게 평가하기 시작할 수 있습니다.

AWS Config 콘솔은 관리형 규칙을 구성하고 활성화하는 프로세스를 안내합니다. AWS Command Line Interface 또는 AWS Config API를 사용하여 관리형 규칙의 구성을 정의하는 JSON 코드를 전달할 수도 있습니다.

관리형 규칙의 동작을 필요에 맞게 사용자 지정할 수 있습니다. 예를 들어, 규칙의 범위를 정의하여 규칙에 대한 평가를 트리거하는 리소스(예: EC2 인스턴스 또는 볼륨)를 제한할 수 있습니다.

규칙의 파라미터를 사용자 지정하여 리소스가 규칙을 준수하기 위해 보유해야 하는 속성을 정의할 수 있습니다. 예를 들어, 보안 그룹이 특정 포트 번호로 들어오는 트래픽을 차단하도록 파라미터를 사용자 지정할 수 있습니다.

관리형 규칙을 사용하기 전에 섹션을 참조하세요고려 사항.

주제

- AWS Config 관리형 규칙 목록
- 평가 모드별 AWS Config 관리형 규칙 목록
- 트리거 유형별 AWS Config 관리형 규칙 목록
- 리전 가용성별 AWS Config 관리형 규칙 목록
- AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성

AWS Config 관리형 규칙 목록

AWS Config 는 현재 다음과 같은 관리형 규칙을 지원합니다. 이러한 규칙을 사용하기 전에 섹션을 참조하세요고려 사항.

주제

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm

- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-ct-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled

- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging

- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururreviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check

- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted

- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled

- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-systems-manager
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description

- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-force-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check

- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-saml-provider-tagged
- iam-server-certificate-expiration-check
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- restricted-ssh
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-standard-scan-enabled
- ec2-instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged

- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled

- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit

- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-common-ports
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3express-dir-bucket-lifecycle-rules-check

- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged

- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access

- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports

- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

access-keys-rotated

유효한 IAM 액세스 키가 `maxAccessKeyAge`에 지정된 일수에 따라 교체(변경)되는지 확인합니다. 지정된 기간 내에 액세스 키가 교체되지 않는 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

> **Warning**
>
> 계정 식별자를 찾는 데 도움이 되더라도 액세스 키를 권한 없는 당사자에게 제공하지 마세요. 이로 인해 다른 사람에게 계정에 대한 영구 액세스를 제공하게 될 수 있습니다. 보안 모범 사례는 사용자에게 암호와 액세스 키가 필요하지 않을 때 그것들을 제거하는 것입니다.

> **Note**
>
> 콘솔에서 규정 미준수로 표시된 리소스 유형
> 이 규칙에서 액세스 키 중 하나라도 규정을 준수하지 않는 것으로 확인되면 AWS 콘솔에서 `AWS::IAM::User` 리소스 유형도 규정을 준수하지 않는 것으로 표시됩니다.

관리형 규칙 및 글로벌 IAM 리소스 유형
2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사용 가능한 AWS 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 리소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에서는 기록할 수 없습니다. 이러한 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.
주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.
불필요한 평가를 방지하려면 지원되는 리전 중 하나에만 글로벌 IAM 리소스 유형에 대해 규정 준수를 보고하는 주기적 규칙을 배포해야 합니다. 리전에서 지원되는 관리형 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.
제한 사항
이 규칙은 AWS 계정 루트 사용자 액세스 키에는 적용되지 않습니다. 루트 사용자 액세스 키를 삭제하거나 교체하려면 루트 사용자 자격 증명을 사용하여 AWS Management Console 의에서 내 보안 자격 증명 페이지에 로그인합니다https://aws.amazon.com/console/.

식별자: ACCESS_KEYS_ROTATED

리소스 유형: AWS::IAM::User

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

maxAccessKeyAge, 유형: int, 기본값: 90

교체가 없는 최대 일수입니다. 기본값: 90.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

account-part-of-organizations

AWS 계정이 AWS Organizations의 일부인지 확인합니다. AWS 계정이 AWS Organizations에 속하지 않거나 AWS Organizations 마스터 계정 ID가 규칙 파라미터와 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다`MasterAccountId`.

> **Note**
>
> 관리형 규칙 및 글로벌 IAM 리소스 유형
> 2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사용 가능한 AWS 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 리소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에서는 기록할 수 없습니다. 이러한 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.
> 주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.
> 불필요한 평가를 방지하려면 지원되는 리전 중 하나에만 글로벌 IAM 리소스 유형에 대해 규정 준수를 보고하는 주기적 규칙을 배포해야 합니다. 리전에서 지원되는 관리형 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.

식별자: ACCOUNT_PART_OF_ORGANIZATIONS

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

MasterAccountId(선택 사항), 유형: 문자열

계정의 마스터 AWS 계정 ID입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

acmpca-certificate-authority-tagged

AWS Private CA 인증 기관에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: ACMPCA_CERTIFICATE_AUTHORITY_TAGGED

리소스 유형: AWS::ACMPCA::CertificateAuthority

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

acm-certificate-expiration-check

계정의 AWS Certificate Manager 인증서가 지정된 일수 내에 만료되도록 표시되어 있는지 확인합니다. ACM이 제공하는 인증서는 자동으로 갱신됩니다. ACM은 사용자가 가져오는 인증서를 자동으로 갱신하지 않습니다. 인증서 만료가 임박한 경우 규칙은 NON_COMPLIANT입니다.

식별자: ACM_CERTIFICATE_EXPIRATION_CHECK

리소스 유형: AWS::ACM::Certificate

트리거 유형: 구성 변경 및 주기적

AWS 리전: 아시아 태평양(오사카) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

daysToExpiration(선택 사항), 유형: int, 기본값: 14

규칙이 ACM 인증서를 규정 미준수로 표시하기까지 남은 일수를 지정합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

acm-certificate-rsa-check

AWS Certificate Manager(ACM)에서 관리하는 RSA 인증서의 키 길이가 '2048'비트 이상인지 확인합니다. 최소 키 길이가 2048비트 미만인 경우 규칙은 NON_COMPLIANT입니다.

식별자: ACM_CERTIFICATE_RSA_CHECK

리소스 유형: AWS::ACM::Certificate

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

acm-pca-root-ca-disabled

AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.

식별자: ACM_PCA_ROOT_CA_DISABLED

리소스 유형: AWS::ACMPCA::CertificateAuthority

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

exemptedCAArns(선택 사항), 유형: CSV

> 활성화할 수 있는 CA의 Amazon 리소스 이름(ARN)을 쉼표로 구분한 목록입니다. 이 값은 활성화할 수 있는 특정 루트 CA 또는 중간 CA 같은 다른 CA에 제공할 수 있습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

active-mq-supported-version

Amazon MQ ActiveMQ 브로커가 지정된 최소 지원 엔진 버전에서 실행 중인지 확인합니다. ActiveMQ 브로커가 지정한 지원되는 최소 엔진 버전에서 실행되지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: ACTIVE_MQ_SUPPORTED_VERSION

리소스 유형: AWS::AmazonMQ::Broker

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

supportedEngineVersion, 유형: 문자열

> ActiveMQ 브로커를 지원하는 최소 엔진 버전을 확인하는 규칙의 문자열 값입니다. ActiveMQ 브로커는 의미 체계 버전 지정 사양(X.Y.Z)을 사용합니다. X는 메이저 버전, Y는 마이너 버전, Z는 패치 버전을 의미합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

alb-desync-mode-check

Application Load Balancer(ALB)가 사용자 정의 비동기화 완화 모드로 구성되어 있는지 확인합니다. ALB 비동기화 완화 모드가 사용자 정의 비동기화 완화 모드와 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

식별자: ALB_DESYNC_MODE_CHECK

리소스 유형: AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

desyncMode, 유형: CSV

> 쉼표로 구분된 목록으로, 고객은 '방어적', '가장 엄격', '모니터링' 중에서 최대 2개의 값을 선택할 수 있습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

alb-http-drop-invalid-header-enabled

규칙이 AWS Application Load Balancer(ALB)를 평가하여 http 헤더를 삭제하도록 구성되어 있는지 확인합니다. routing.http.drop_invalid_header_fields.enabled 값이 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: ALB_HTTP_DROP_INVALID_HEADER_ENABLED

리소스 유형: AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(오사카) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

alb-http-to-https-redirection-check

Application Load Balancer의 모든 HTTP 리스너에 HTTP-HTTPS 리디렉션이 구성되어 있는지 확인합니다. Application Load Balancer의 HTTP 리스너 중 하나 이상에 HTTP-HTTPS 리디렉션이 구성되어 있지 않으면 규칙은 NON_COMPLIANT입니다. 하나 이상의 HTTP 리스너가 리디렉션 대신 HTTP 리스너로 전달하는 경우에도 규칙은 NON_COMPLIANT입니다.

식별자: ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

리소스 유형: AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 유형: 주기적

AWS 리전: 아시아 태평양(오사카) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

alb-internal-scheme-check

Application Load Balancer 체계가 내부인지 확인합니다. configuration.scheme이 내부로 설정되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: ALB_INTERNAL_SCHEME_CHECK

리소스 유형: AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

alb-listener-tagged

Application Load Balancer 리스너에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: ALB_LISTENER_TAGGED

리소스 유형: AWS::ElasticLoadBalancingV2::Listener

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

alb-waf-enabled

Application Load Balancer(ALBs)에서 AWS WAF가 활성화되어 있는지 확인합니다. key: waf.enabled가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: ALB_WAF_ENABLED

리소스 유형: AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(오사카) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

wafWebAclIds(선택 사항), 유형: CSV

ALB 연결을 확인하는 쉼표로 구분된 웹 ACL ID(WAF용) 또는 웹 ACL ARN(WAFV2용) 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

amplify-app-branch-auto-deletion-enabled

Git 리포지토리에서 브랜치를 삭제할 때 AWS Amplify 앱이 Amplify Hosting의 브랜치를 자동으로 연결 해제하는지 확인합니다. configuration.EnableBranchAutoDeletion이 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: AMPLIFY_APP_BRANCH_AUTO_DELETION_ENABLED

리소스 유형: AWS::Amplify::App

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS

GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

amplify-app-description

AWS Amplify 앱에 설명이 있는지 확인합니다. configuration.Description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: AMPLIFY_APP_DESCRIPTION

리소스 유형: AWS::Amplify::App

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

amplify-app-tagged

AWS Amplify 앱에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: AMPLIFY_APP_TAGGED

리소스 유형: AWS::Amplify::App

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

amplify-branch-performance-mode-enabled

AWS Amplify 브랜치에 성능 모드가 활성화되어 있는지 확인합니다. configuration.EnablePerformanceMode가 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: AMPLIFY_BRANCH_PERFORMANCE_MODE_ENABLED

리소스 유형: AWS::Amplify::Branch

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

amplify-branch-tagged

AWS Amplify 브랜치에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: AMPLIFY_BRANCH_TAGGED

리소스 유형: AWS::Amplify::Branch

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

api-gwv2-access-logs-enabled

Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: API_GWV2_ACCESS_LOGS_ENABLED

리소스 유형: AWS::ApiGatewayV2::Stage

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

api-gwv2-authorization-type-configured

Amazon API Gatewayv2 API 경로에 권한 부여 유형이 설정되어 있는지 확인합니다. 권한 부여 유형이 NONE인 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: API_GWV2_AUTHORIZATION_TYPE_CONFIGURED

리소스 유형: AWS::ApiGatewayV2::Route

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

authorizationType(선택 사항), 유형: 문자열

> API 경로의 권한 부여 유형을 확인하기 위한 파라미터입니다. CUSTOM, AWS_IAM, JWT와 일치하는 문자열 파라미터가 유효합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

api-gw-associated-with-waf

Amazon API Gateway API 단계에서 AWS WAF 웹 액세스 제어 목록(웹 ACL)을 사용하고 있는지 확인합니다. AWS WAF 웹 ACL을 사용하지 않거나 사용된 AWS 웹 ACL이 규칙 파라미터에 나열된 것과 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: API_GW_ASSOCIATED_WITH_WAF

리소스 유형: AWS::ApiGateway::Stage

트리거 0유형: 구성 변경

AWS 리전: 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

WebAclArns(선택 사항), 유형: CSV

웹 ACL 아마존 리소스 이름(ARN)을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

api-gw-cache-enabled-and-encrypted

Amazon API Gateway 단계의 모든 메서드에 캐시가 활성화되어 있고 캐시가 암호화되어 있는지 확인합니다. Amazon API Gateway 단계에 캐싱이 구성되지 않았거나, 캐시가 암호화되지 않은 메서드가 있을 경우 규칙은 NON_COMPLIANT입니다.

식별자: API_GW_CACHE_ENABLED_AND_ENCRYPTED

리소스 유형: AWS::ApiGateway::Stage

트리거 0유형: 구성 변경

AWS 리전: 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

api-gw-endpoint-type-check

Amazon API Gateway API가 규칙 파라미터 `endpointConfigurationType`에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.

식별자: API_GW_ENDPOINT_TYPE_CHECK

리소스 유형: AWS::ApiGateway::RestApi

트리거 0유형: 구성 변경

AWS 리전: 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

endpointConfigurationTypes, 유형: 문자열

허용되는 endpointConfigurationTypes를 쉼표로 구분한 목록입니다. 허용된 값은 REGIONAL, PRIVATE 및 EDGE입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

api-gw-execution-logging-enabled

Amazon API Gateway 단계의 모든 메서드에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 `loggingLevel`이 ERROR 또는 INFO가 아닌 경우 규칙은 NON_COMPLIANT입니다.

식별자: API_GW_EXECUTION_LOGGING_ENABLED

리소스 유형: AWS::ApiGateway::Stage, AWS::ApiGatewayV2::Stage

트리거 0유형: 구성 변경

AWS 리전: 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

loggingLevel(선택 사항), 유형: 문자열, 기본값: ERROR,INFO

특정 로깅 수준(예: ERROR, INFO 또는 ERROR,INFO)을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

api-gw-ssl-enabled

REST API 단계가 SSL 인증서를 사용하는지 확인합니다. REST API 단계에 연결된 SSL 인증서가 없는 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> GetIntegration API가 `AWS`를 유형으로 반환할 경우 이 규칙은 `NOT_APPLICABLE`을 반환합니다.

식별자: API_GW_SSL_ENABLED

리소스 유형: AWS::ApiGateway::Stage

트리거 0유형: 구성 변경

AWS 리전: 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

CertificateIDs(선택 사항), 유형: CSV

REST API 단계에서 구성된 클라이언트 인증서 ID를 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

api-gw-xray-enabled

Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

식별자: API_GW_XRAY_ENABLED

리소스 유형: AWS::ApiGateway::Stage

트리거 0유형: 구성 변경

AWS 리전: 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
...
```

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appconfig-application-description

AWS AppConfig 애플리케이션에 설명이 있는지 확인합니다. configuration.Description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPCONFIG_APPLICATION_DESCRIPTION

리소스 유형: AWS::AppConfig::Application

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appconfig-application-tagged

AWS AppConfig 애플리케이션에 태그가 있는지 확인합니다. 선택적으로 확인할 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPCONFIG_APPLICATION_TAGGED

리소스 유형: AWS::AppConfig::Application

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appconfig-configuration-profile-tagged

AWS AppConfig 구성 프로필에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPCONFIG_CONFIGURATION_PROFILE_TAGGED

리소스 유형: AWS::AppConfig::ConfigurationProfile

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appconfig-configuration-profile-validators-not-empty

구성 배포가 의도한 대로 작동하는지 확인하기 위해 AWS AppConfig 구성 프로파일에 구문 또는 의미 확인을 위한 검사기가 하나 이상 포함되어 있는지 확인합니다. 검사기 속성이 빈 배열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPCONFIG_CONFIGURATION_PROFILE_VALIDATORS_NOT_EMPTY

리소스 유형: AWS::AppConfig::ConfigurationProfile

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appconfig-deployment-strategy-description

AWS AppConfig 배포 전략에 설명이 있는지 확인합니다. configuration.Description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPCONFIG_DEPLOYMENT_STRATEGY_DESCRIPTION

리소스 유형: AWS::AppConfig::DeploymentStrategy

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appconfig-deployment-strategy-replicate-to-ssm

AWS AppConfig 배포 전략이 배포 전략을 AWS Systems Manager(SSM) 문서에 저장하는지 확인합니다. configuration.ReplicateTo가 'SSM_DOCUMENT'가 아닌 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPCONFIG_DEPLOYMENT_STRATEGY_REPLICATE_TO_SSM

리소스 유형: AWS::AppConfig::DeploymentStrategy

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appconfig-environment-description

AWS AppConfig 환경에 설명이 있는지 확인합니다. configuration.Description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPCONFIG_ENVIRONMENT_DESCRIPTION

리소스 유형: AWS::AppConfig::Environment

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appconfig-environment-tagged

AWS AppConfig 환경에 태그가 있는지 확인합니다. 선택적으로 확인할 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPCONFIG_ENVIRONMENT_TAGGED

리소스 유형: AWS::AppConfig::Environment

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appconfig-extension-association-tagged

AWS AppConfig 확장 연결에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPCONFIG_EXTENSION_ASSOCIATION_TAGGED

리소스 유형: AWS::AppConfig::ExtensionAssociation

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appconfig-freeform-profile-config-storage

AWS AppConfig의 자유 형식 구성 프로필이 구성 데이터를 AWS Secrets Manager 또는 AWS AppConfig 호스팅 구성 저장소에 저장하는지 확인합니다. configuration.LocationUri가 secretsmanager 또는 호스팅되지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPCONFIG_FREEFORM_PROFILE_CONFIG_STORAGE

리소스 유형: AWS::AppConfig::ConfigurationProfile

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appconfig-hosted-configuration-version-description

AWS AppConfig 호스팅 구성 버전에 설명이 있는지 확인합니다. configuration.Description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPCONFIG_HOSTED_CONFIGURATION_VERSION_DESCRIPTION

리소스 유형: AWS::AppConfig::HostedConfigurationVersion

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appflow-flow-tagged

Amazon AppFlow 흐름에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPFLOW_FLOW_TAGGED

리소스 유형: AWS::AppFlow::Flow

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 아프리카(케이프타운), 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appintegrations-event-integration-description

Amazon AppIntegrations 이벤트 통합에 설명이 있는지 확인합니다. configuration.Description이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPINTEGRATIONS_EVENT_INTEGRATION_DESCRIPTION

리소스 유형: AWS::AppIntegrations::EventIntegration

트리거 0유형: 구성 변경

AWS 리전: 아프리카(케이프타운), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appintegrations-event-integration-tagged

Amazon AppIntegrations 이벤트 통합에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPINTEGRATIONS_EVENT_INTEGRATION_TAGGED

리소스 유형: AWS::AppIntegrations::EventIntegration

트리거 0유형: 구성 변경

AWS 리전: 아프리카(케이프타운), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-gateway-route-tagged

AWS App Mesh 게이트웨이 경로에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPMESH_GATEWAY_ROUTE_TAGGED

리소스 유형: AWS::AppMesh::GatewayRoute

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-mesh-deny-tcp-forwarding

AWS App Mesh 서비스 메시에 대한 프록시가 TCP 트래픽을 메시에 정의된 프록시와 함께 배포되지 않은 서비스로 직접 전달하지 않는지 확인합니다. configuration.Spec.EgressFilter.Type이 'ALLOW_ALL'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPMESH_MESH_DENY_TCP_FORWARDING

리소스 유형: AWS::AppMesh::Mesh

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-mesh-tagged

AWS App Mesh 메시에 태그가 있는지 확인합니다. 선택적으로 확인할 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPMESH_MESH_TAGGED

리소스 유형: AWS::AppMesh::Mesh

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-route-tagged

AWS App Mesh 경로에 태그가 있는지 확인합니다. 선택적으로 확인할 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPMESH_ROUTE_TAGGED

리소스 유형: AWS::AppMesh::Route

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-virtual-gateway-backend-defaults-tls

AWS App Mesh 가상 게이트웨이의 백엔드 기본값에 TLS를 사용하여 가상 게이트웨이가 모든 포트와 통신해야 하는지 확인합니다. configuration.Spec.BackendDefaults.ClientPolicy.Tls.Enforce가 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPMESH_VIRTUAL_GATEWAY_BACKEND_DEFAULTS_TLS

리소스 유형: AWS::AppMesh::VirtualGateway

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-virtual-gateway-logging-file-path-exists

AWS App Mesh 가상 게이트웨이에 액세스 로그를 쓸 파일 경로가 있는지 확인합니다. configuration.Spec.Logging.AccessLog.File.Path가 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPMESH_VIRTUAL_GATEWAY_LOGGING_FILE_PATH_EXISTS

리소스 유형: AWS::AppMesh::VirtualGateway

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-virtual-gateway-tagged

AWS App Mesh 가상 게이트웨이에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPMESH_VIRTUAL_GATEWAY_TAGGED

리소스 유형: AWS::AppMesh::VirtualGateway

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-virtual-node-backend-defaults-tls-on

AWS App Mesh 가상 노드의 백엔드 기본값에 TLS를 사용하여 가상 노드가 모든 포트와 통신해야 하는지 확인합니다. configuration.Spec.BackendDefaults.ClientPolicy.Tls.Enforce가 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPMESH_VIRTUAL_NODE_BACKEND_DEFAULTS_TLS_ON

리소스 유형: AWS::AppMesh::VirtualNode

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-virtual-node-logging-file-path-exists

AWS App Mesh 가상 노드에 액세스 로그를 쓸 파일 경로가 있는지 확인합니다. configuration.Spec.Logging.AccessLog.File.Path가 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPMESH_VIRTUAL_NODE_LOGGING_FILE_PATH_EXISTS

리소스 유형: AWS::AppMesh::VirtualNode

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-virtual-node-tagged

AWS App Mesh 가상 노드에 태그가 있는지 확인합니다. 선택적으로 확인할 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPMESH_VIRTUAL_NODE_TAGGED

리소스 유형: AWS::AppMesh::VirtualNode

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-virtual-router-tagged

AWS App Mesh 가상 라우터에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPMESH_VIRTUAL_ROUTER_TAGGED

리소스 유형: AWS::AppMesh::VirtualRouter

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appmesh-virtual-service-tagged

AWS App Mesh 가상 서비스에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPMESH_VIRTUAL_SERVICE_TAGGED

리소스 유형: AWS::AppMesh::VirtualService

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

approved-amis-by-id

EC2 인스턴스가 지정된 Amazon Machine Image(AMIs 사용하고 있는지 확인합니다. 승인된 AMI ID 목록을 지정합니다. 실행 중인 인스턴스 중 이 목록에 없는 AMI를 사용하는 인스턴스는 NON_COMPLIANT로 간주됩니다.

식별자: APPROVED_AMIS_BY_ID

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

amiIds, 유형: CSV

최대 21개의 AMI IDs. 1024자로 제한됩니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

approved-amis-by-tag

EC2 인스턴스가 지정된 Amazon Machine Image(AMIs 사용하고 있는지 확인합니다. AMI를 식별하는 태그를 지정합니다. 실행 중인 인스턴스 중, 하나 이상의 지정 태그가 없는 AMI를 사용하는 인스턴스는 NON_COMPLIANT로 간주됩니다.

식별자: APPROVED_AMIS_BY_TAG

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

amisByTagKeyAndValue, 유형: StringMap, 기본값: tag-key:tag-value,other-tag-key

최대 10개의 AMIs 태그(tag-key:tag-value)로 구성된 쉼표로 구분된 목록입니다. 예를 들어 tag-key1은 AMIs tag-key1과 일치시키고 tag-key2:value2는 tag-key2를 값 2와 일치시킵니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

apprunner-service-in-vpc

AWS App Runner 서비스가 사용자 지정 VPC를 통해 송신 트래픽을 라우팅하는지 확인합니다. configuration.NetworkConfiguration.EgressConfiguration.EgressType이 DEFAULT인 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPRUNNER_SERVICE_IN_VPC

리소스 유형: AWS::AppRunner::Service

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

apprunner-service-no-public-access

AWS AppRunner Services에 공개적으로 액세스할 수 없는지 확인합니다. service.configuration.NetworkConfiguration.IngressConfiguration.IsPubliclyAccessible이 False인 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPRUNNER_SERVICE_NO_PUBLIC_ACCESS

리소스 유형: AWS::AppRunner::Service

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

apprunner-service-observability-enabled

AWS App Runner 서비스에 관찰성이 활성화되어 있는지 확인합니다. configuration.ObservabilityConfiguration.ObservabilityEnabled가 false'인 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPRUNNER_SERVICE_OBSERVABILITY_ENABLED

리소스 유형: AWS::AppRunner::Service

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

apprunner-service-tagged

AWS App Runner 서비스에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPRUNNER_SERVICE_TAGGED

리소스 유형: AWS::AppRunner::Service

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

apprunner-vpc-connector-tagged

AWS App Runner VPC 커넥터에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: APPRUNNER_VPC_CONNECTOR_TAGGED

리소스 유형: AWS::AppRunner::VpcConnector

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appstream-fleet-in-vpc

Amazon AppStream 2.0 플릿이 Amazon Virtual Private Cloud(Amazon VPC)를 사용하는지 확인합니다. configuration.VpcConfig가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 탄력적 플릿을 확인하지 않습니다.

식별자: APPSTREAM_FLEET_IN_VPC

리소스 유형: AWS::AppStream::Fleet

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appsync-associated-with-waf

AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙이 웹 ACL과 연결되지 않은 경우 AWS AppSync API에 대한 규칙은 NON_COMPLIANT입니다.

식별자: APPSYNC_ASSOCIATED_WITH_WAF

리소스 유형: AWS::AppSync::GraphQLApi

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

wafWebAclARNs(선택 사항), 유형: CSV

승인된 웹 ACL에 대한 Amazon 리소스 이름(ARN)을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appsync-authorization-check

AWS AppSync API가 허용된 권한 부여 메커니즘을 사용하고 있는지 확인합니다. 승인되지 않은 권한 부여 메커니즘을 사용할 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPSYNC_AUTHORIZATION_CHECK

리소스 유형: AWS::AppSync::GraphQLApi

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

AllowedAuthorizationTypes, 유형: CSV

쉼표로 구분된 allowed AWS AppSync 권한 부여 메커니즘 목록입니다. 허용되는 값은 'API_KEY', 'AWS_LAMBDA', 'AWS_IAM', 'OPENID_CONNECT', 'AMAZON_COGNITO_USER_POOLS'입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appsync-cache-ct-encryption-at-rest

AWS AppSync API 캐시에 저장 시 암호화가 활성화되어 있는지 확인합니다. 'AtRestEncryptionEnabled'가 false인 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: APPSYNC_CACHE_CT_ENCRYPTION_AT_REST

리소스 유형: AWS::AppSync::ApiCache

트리거 0유형: 구성 변경

AWS 리전: 중동(바레인), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appsync-cache-ct-encryption-in-transit

AWS AppSync API 캐시에 전송 중 암호화가 활성화되어 있는지 확인합니다. 'TransitEncryptionEnabled'가 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPSYNC_CACHE_CT_ENCRYPTION_IN_TRANSIT

리소스 유형: AWS::AppSync::ApiCache

트리거 0유형: 구성 변경

AWS 리전: 중동(바레인), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appsync-cache-encryption-at-rest

AWS AppSync API 캐시에 저장 시 암호화가 활성화되어 있는지 확인합니다. 'AtRestEncryptionEnabled'가 false인 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: APPSYNC_CACHE_ENCRYPTION_AT_REST

리소스 유형: AWS::AppSync::GraphQLApi

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

appsync-logging-enabled

AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않았거나 AWS AppSync API의 필드 로깅 수준이 `'fieldLoggingLevel'` 규칙 파라미터에 지정된 값과 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: APPSYNC_LOGGING_ENABLED

리소스 유형: AWS::AppSync::GraphQLApi

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

fieldLoggingLevel(선택 사항), 유형: CSV

확인할 규칙에 대한 필드 로깅 수준의 쉼표로 구분된 목록입니다. 예: "오류, 정보".

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

athena-data-catalog-description

Amazon Athena 데이터 카탈로그에 설명이 있는지 확인합니다. configuration.Description이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: ATHENA_DATA_CATALOG_DESCRIPTION

리소스 유형: AWS::Athena::DataCatalog

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

athena-prepared-statement-description

Amazon Athena에서 준비한 문에 설명이 있는지 확인합니다. configuration.Description이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: ATHENA_PREPARED_STATEMENT_DESCRIPTION

리소스 유형: AWS::Athena::PreparedStatement

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

athena-workgroup-description

Amazon Athena 작업 그룹에 설명이 있는지 확인합니다. configuration.Description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: ATHENA_WORKGROUP_DESCRIPTION

리소스 유형: AWS::Athena::WorkGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

athena-workgroup-encrypted-at-rest

Amazon Athena 작업 그룹이 저장 시 암호화되는지 확인합니다. Athena 작업 그룹에 대해 저장 데이터 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: ATHENA_WORKGROUP_ENCRYPTED_AT_REST

리소스 유형: AWS::Athena::WorkGroup

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

athena-workgroup-enforce-workgroup-configuration

Athena 엔진을 사용하는 Amazon Athena 작업 그룹이 작업 그룹 구성을 적용하여 클라이언트 측 설정을 재정의하는지 확인합니다. configuration.WorkGroupConfiguration.EnforceWorkGroupConfiguration이 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: ATHENA_WORKGROUP_ENFORCE_WORKGROUP_CONFIGURATION

리소스 유형: AWS::Athena::WorkGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

athena-workgroup-engine-version-auto-upgrade

Athena 엔진을 사용하는 Amazon Athena 작업 그룹이 자동 업그레이드하도록 구성되어 있는지 확인합니다. configuration.WorkGroupConfiguration.EngineVersion.SelectedEngineVersion이 'AUTO'가 아닌 경우 규칙은 NON_COMPLIANT입니다.

식별자: ATHENA_WORKGROUP_ENGINE_VERSION_AUTO_UPGRADE

리소스 유형: AWS::Athena::WorkGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

athena-workgroup-logging-enabled

Amazon Athena 작업 그룹이 사용량 지표를 Amazon CloudWatch에 게시하는지 확인합니다. Amazon Athena WorkGroup 'PublishCloudWatchMetricsEnabled'가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: ATHENA_WORKGROUP_LOGGING_ENABLED

리소스 유형: AWS::Athena::WorkGroup

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

aurora-last-backup-recovery-point-created

Amazon Aurora DB 클러스터에 대한 복구 시점이 생성되었는지 확인합니다. Amazon Relational Database Service(RDS) DB 클러스터에 지정된 기간 내에 생성된 해당 복구 시점이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED

리소스 유형: AWS::RDS::DBCluster

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Aurora DB 클러스터의 태그입니다(JSON 형식 `{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Aurora DB 클러스터의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 744시간, 일수는 31일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

aurora-meets-restore-time-target

Amazon Aurora DB 클러스터의 복원 시간이 지정된 기간을 충족하는지 확인합니다. Amazon Aurora DB 클러스터의 LatestRestoreExecutionTimeMinutes가 maxRestoreTime(분)보다 큰 경우 규칙은 NON_COMPLIANT입니다.

식별자: AURORA_MEETS_RESTORE_TIME_TARGET

리소스 유형: AWS::RDS::DBCluster

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

maxRestoreTime, 유형: int

허용되는 최대 복원 런타임의 숫자 값입니다.

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Aurora DB 클러스터의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Aurora DB 클러스터의 ID입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

aurora-mysql-backtracking-enabled

Amazon Aurora MySQL 클러스터에 백트래킹이 활성화되어 있는지 확인합니다. Aurora 클러스터가 MySQL을 사용하며 역추적이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: AURORA_MYSQL_BACKTRACKING_ENABLED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 중동(바레인), 중국(베이징), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 남아메리카(상파울루), 아시아 태평양(홍콩), 아시아 태평양(하이데라바드), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

BacktrackWindowInHours(선택 사항), 유형: double

Aurora MySQL 클러스터를 역추적하는 데 걸리는 시간(최대 72시간)입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

aurora-mysql-cluster-audit-logging

Amazon Aurora MySQL DB 클러스터에 감사 로깅이 활성화되어 있는지 확인합니다. DB 클러스터에 감사 로깅이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: AURORA_MYSQL_CLUSTER_AUDIT_LOGGING

리소스 유형: AWS::RDS::DBCluster

트리거 유형: 주기적

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

aurora-resources-in-logically-air-gapped-vault

Amazon Aurora DB 클러스터가 논리적 에어 갭 저장소에 있는지 확인합니다. Amazon Aurora DB 클러스터가 지정된 기간 내에 논리적 에어 갭 저장소에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: AURORA_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

리소스 유형: AWS::RDS::DBCluster

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Aurora DB 클러스터의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Aurora DB 클러스터의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 2184시간, 일수는 91일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

aurora-resources-protected-by-backup-plan

Amazon Aurora DB 클러스터가 백업 계획에 의해 보호되고 있는지 확인합니다. Amazon Relational Database Service(RDS) 데이터베이스 클러스터가 백업 계획에 의해 보호되고 있지 않을 경우 규칙은 NON_COMPLIANT입니다.

식별자: AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN

리소스 유형: AWS::RDS::DBCluster

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Aurora DB 클러스터의 태그입니다(JSON 형식 `{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Aurora DB 클러스터의 ID입니다.

crossRegionList(선택 사항), 유형: 문자열

리전 간 백업 사본을 보관할 대상 리전을 쉼표로 구분한 목록입니다.

crossAccountList(선택 사항), 유형: 문자열

계정 간 백업 사본을 보관할 대상 계정을 쉼표로 구분한 목록입니다.

maxRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최대 보존 기간(일)

minRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최소 보존 기간(일)

backupVaultLockCheck(선택 사항), 유형: 문자열

허용되는 값: 'True' 또는 'False'. 리소스가 잠긴 볼트에 백업되어 있는지 확인하는 규칙에 'True'를 입력합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

autoscaling-capacity-rebalancing

여러 인스턴스 유형을 사용하는 Amazon EC2 Auto Scaling 그룹에 대해 용량 재조정이 활성화되어 있음을 확인합니다. 용량 재조정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: AUTOSCALING_CAPACITY_REBALANCING

리소스 유형: AWS::AutoScaling::AutoScalingGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

autoscaling-group-elb-healthcheck-required

Elastic Load Balancer와 연결된 Amazon EC2 Auto Scaling 그룹이 Elastic Load Balancing 상태 확인을 사용하고 있는지 확인합니다. Amazon EC2 Auto Scaling 그룹에서 Elastic Load Balancing 상태 확인 기능을 사용하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

리소스 유형: AWS::AutoScaling::AutoScalingGroup

트리거 0유형: 구성 변경

AWS 리전: 중동(UAE), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-
balancer-3, ...]",
   "HealthCheckType": HealthCheckType*"
}
...
```

*유효한 값은 EC2(기본값), ELB, VPC_LATTICE입니다. VPC_LATTICE 상태 점검 유형은 평가판 릴리스 중이며 변경될 수 있는 VPC Lattice와 함께 사용하도록 예약되었습니다. 자세한 내용은 Amazon EC2 Auto Scaling 사용 설명서의 Auto Scaling 인스턴스에 대한 상태 확인 섹션을 참조하세요.

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

autoscaling-launchconfig-requires-imdsv2

IMDSv2만 활성화되어 있는지 확인합니다. 메타데이터 버전이 시작 구성에 포함되어 있지 않거나, 메타데이터 V1과 V2가 둘 다 활성화된 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2

리소스 유형: AWS::AutoScaling::LaunchConfiguration

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

autoscaling-launch-config-hop-limit

메타데이터 토큰이 이동할 수 있는 네트워크 홉 수를 확인합니다. 메타데이터 응답 홉 제한이 1보다 큰 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

리소스 유형: AWS::AutoScaling::LaunchConfiguration

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

autoscaling-launch-config-public-ip-disabled

Amazon EC2 Auto Scaling 그룹에 시작 구성을 통해 활성화된 퍼블릭 IP 주소가 있는지 확인합니다. Amazon EC2 Auto Scaling 그룹의 시작 구성에 AssociatePublicIpAddress가 'true'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

리소스 유형: AWS::AutoScaling::LaunchConfiguration

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

autoscaling-launch-template

Amazon Elastic Compute Cloud(EC2) Auto Scaling 그룹이 EC2 시작 템플릿으로 생성되었는지 확인합니다. EC2 시작 템플릿에서 스케일링 그룹을 생성하지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: AUTOSCALING_LAUNCH_TEMPLATE

리소스 유형: AWS::AutoScaling::AutoScalingGroup

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

autoscaling-multiple-az

Auto Scaling 그룹이 여러 가용 영역에 걸쳐 있는지 확인합니다. Auto Scaling 그룹이 여러 가용 영역에 걸쳐 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: AUTOSCALING_MULTIPLE_AZ

리소스 유형: AWS::AutoScaling::AutoScalingGroup

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

minAvailabilityZones(선택 사항), 유형: int

예상 가용 영역의 최소 수입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

autoscaling-multiple-instance-types

Amazon EC2 Auto Scaling 그룹이 여러 인스턴스 유형을 사용하는지 확인합니다. Amazon EC2 Auto Scaling 그룹에 인스턴스 유형이 하나만 정의된 경우 규칙은 NON_COMPLIANT입니다. 이 규칙은 속성 기반 인스턴스 유형을 평가하지 않습니다.

식별자: AUTOSCALING_MULTIPLE_INSTANCE_TYPES

리소스 유형: AWS::AutoScaling::AutoScalingGroup

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

backup-plan-min-frequency-and-min-retention-check

백업 계획에 필수 빈도 및 보존 기간을 충족하는 백업 규칙이 있는지 확인합니다. 복구 시점이 지정된 빈도만큼 자주 생성되지 않거나 지정된 기간 이전에 만료되는 경우 규칙은 NON_COMPLIANT입니다.

식별자: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

리소스 유형: AWS::Backup::BackupPlan

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredFrequencyValue(선택 사항), 유형: int, 기본값: 1

필수 백업 빈도의 숫자 값입니다. 최대값은 시간은 24시간, 일은 31일입니다.

requiredRetentionDays(선택 사항), 유형: int, 기본값: 35

필수 보존 기간(일 단위)입니다.

requiredFrequencyUnit(선택 사항), 유형: 문자열, 기본값: 일

필수 백업 빈도의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

backup-recovery-point-encrypted

복구 시점이 암호화되어 있는지 확인합니다. 복구 시점이 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: BACKUP_RECOVERY_POINT_ENCRYPTED

리소스 유형: AWS::Backup::RecoveryPoint

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

backup-recovery-point-manual-deletion-disabled

백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 거부 문의 **`"Resource"`** 및 **`"Principal"`**에 필요한 와일드카드
>
> 규칙에서는 거부 문의 `"Resource"` 및 `"Principal"`에 볼트 액세스 정책에 와일드카드가 있어야 합니다. 그렇지 않으면 규칙이 NON_COMPLIANT를 반환합니다.

식별자: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED

리소스 유형: AWS::Backup::BackupVault

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

principalArnList(선택 사항), 유형: CSV

확인하지 않을 규칙에 대한 AWS ID 및 액세스 관리(IAM) Amazon 리소스 이름(ARNs)의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

backup-recovery-point-minimum-retention-check

지정된 기간 이후보다 복구 시점이 더 빨리 만료되지 않는지 확인합니다. 복구 시점의 보존 시점이 필수 보존 기간보다 짧은 경우 규칙은 NON_COMPLIANT입니다.

식별자: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK

리소스 유형: AWS::Backup::RecoveryPoint

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredRetentionDays(선택 사항), 유형: int, 기본값: 35

필수 보존 기간(일 단위)입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

batch-compute-environment-enabled

AWS 배치 컴퓨팅 환경이 활성화되어 있는지 확인합니다. configuration.State가 'DISABLED'인 경우 규칙은 NON_COMPLIANT입니다.

식별자: BATCH_COMPUTE_ENVIRONMENT_ENABLED

리소스 유형: AWS::Batch::ComputeEnvironment

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

batch-compute-environment-managed

AWS 배치 컴퓨팅 환경이 관리되는지 확인합니다. configuration.Type이 'UNMANAGED'인 경우 규칙은 NON_COMPLIANT입니다.

식별자: BATCH_COMPUTE_ENVIRONMENT_MANAGED

리소스 유형: AWS::Batch::ComputeEnvironment

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

batch-compute-environment-tagged

AWS 배치 컴퓨팅 환경에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: BATCH_COMPUTE_ENVIRONMENT_TAGGED

리소스 유형: AWS::Batch::ComputeEnvironment

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

batch-job-queue-enabled

AWS 배치 작업 대기열이 활성화되어 있는지 확인합니다. configuration.State가 'DISABLED'인 경우 규칙은 NON_COMPLIANT입니다.

식별자: BATCH_JOB_QUEUE_ENABLED

리소스 유형: AWS::Batch::JobQueue

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

batch-job-queue-tagged

AWS 배치 작업 대기열에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: BATCH_JOB_QUEUE_TAGGED

리소스 유형: AWS::Batch::JobQueue

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

batch-managed-compute-environment-using-launch-template

시작 템플릿을 사용하여 AWS 배치 관리형 컴퓨팅 환경이 구성되어 있는지 확인합니다. configuration.ComputeResources.LaunchTemplate이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: BATCH_MANAGED_COMPUTE_ENVIRONMENT_USING_LAUNCH_TEMPLATE

리소스 유형: AWS::Batch::ComputeEnvironment

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

batch-managed-compute-env-compute-resources-tagged

AWS 배치 관리형 컴퓨팅 환경 컴퓨팅 리소스에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 'aws:'로 시작하는 태그는 선택되지 않습니다.

식별자: BATCH_MANAGED_COMPUTE_ENV_COMPUTE_RESOURCES_TAGGED

리소스 유형: AWS::Batch::ComputeEnvironment

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

batch-scheduling-policy-tagged

AWS 배치 예약 정책에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: BATCH_SCHEDULING_POLICY_TAGGED

리소스 유형: AWS::Batch::SchedulingPolicy

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

beanstalk-enhanced-health-reporting-enabled

AWS Elastic Beanstalk 환경이 향상된 상태 보고를 위해 구성되어 있는지 확인합니다. 환경이 향상된 상태 보고를 위해 구성되어 있는 경우 규칙은 COMPLIANT입니다. 환경이 기본 상태 보고를 위해 구성되어 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

리소스 유형: AWS::ElasticBeanstalk::Environment

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cassandra-keyspace-tagged

Amazon Keyspaces(Apache Cassandra용) 키스페이스에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: CASSANDRA_KEYSPACE_TAGGED

리소스 유형: AWS::Cassandra::Keyspace

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 중동(바레인), 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 아시아 태평양(홍콩), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

clb-desync-mode-check

Classic Load Balancer(CLB)가 사용자 정의 비동기화 완화 모드로 구성되어 있는지 확인합니다. CLB 비동기화 완화 모드가 사용자 정의 비동기화 완화 모드와 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLB_DESYNC_MODE_CHECK

리소스 유형: AWS::ElasticLoadBalancing::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

desyncMode, 유형: CSV

> 쉼표로 구분된 값 목록입니다. 최대 두 개를 선택할 수 있습니다. 유효한 값에는 '방어적', '가장 엄격', '모니터링'이 포함됩니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

clb-multiple-az

Classic Load Balancer가 여러 가용 영역(AZ)에 걸쳐 있는지 확인합니다. Classic Load Balancer가 2개 이하의 AZ에 걸쳐 있거나, `minAvailabilityZones` 파라미터(제공된 경우)에 언급된 여러 AZ에 걸쳐 있지 않으면 규칙은 NON_COMPLIANT입니다.

식별자: CLB_MULTIPLE_AZ

리소스 유형: AWS::ElasticLoadBalancing::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

minAvailabilityZones(선택 사항), 유형: int

> 원하는 최소 예상 AZ 수입니다. 유효한 값은 2~10 사이입니다. 파라미터가 지정되지 않을 경우 기본값은 2입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudformation-stack-drift-detection-check

AWS CloudFormation (AWS CloudFormation) 스택의 실제 구성이 예상 구성과 다른지 또는 드리프트되었는지 확인합니다. 스택은 하나 이상의 리소스가 해당 리소스에 요구되는 구성과 다를 경우 드리프트된 것으로 간주됩니다. 스택의 드리프트 상태가 IN_SYNC인 경우 규칙과 스택은 COMPLIANT로 간주됩니다. 스택의 드리프트 상태가 DRIFTED인 경우 규칙은 NON_COMPLIANT로 간주됩니다.

> **Note**
>
> 이 규칙은 계정의 각 스택에서 DetectStackDrift 작업을 수행합니다. DetectStackDrift 작업은 몇 분이 걸릴 수 있으며, 스택에 포함된 리소스의 수에 따라 다릅니다. 이 규칙의 최대 실행 시간은 15분으로 제한되므로, 계정 내의 모든 스택에 대한 평가를 완료하기 전에 규칙 제한 시간이 초과될 수 있습니다.
> 이러한 문제가 발생할 경우 태그를 사용하여 규칙의 범위 내 스택 수를 제한하는 것이 좋습니다. 다음을 수행할 수 있습니다.
>
> 1. 스택을 각각 다른 태그가 있는 그룹으로 나눕니다.
> 2. 해당 그룹의 모든 스택에 동일한 태그를 적용합니다.
> 3. 계정에서 이 규칙의 인스턴스를 여러 개 보유합니다. 각 인스턴스는 다른 태그로 범위를 지정해야 합니다. 이렇게 하면 규칙의 각 인스턴스는 범위 내에서 해당 태그가 언급된 스택만 처리할 수 있습니다.

식별자: CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

리소스 유형: AWS::CloudFormation::Stack

트리거 유형: 구성 변경 및 주기적

AWS 리전: 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(멜버른), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

cloudformationRoleArn, 유형: 문자열

AWS CloudFormation 스택의 드리프트를 감지할 수 있는 정책 권한이 있는 IAM 역할의 Amazon 리소스 이름(ARN)입니다. 역할에 필요한 IAM 권한에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 스택 및 리소스에 대한 비관리형 구성 변경 감지 | 드리프트 감지 시 고려 사항을 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudformation-stack-notification-check

CloudFormation 스택이 Amazon SNS 주제로 이벤트 알림을 전송하는지 확인합니다. 필요한 경우 특정 Amazon SNS 주제가 사용되는지 여부를 확인합니다. CloudFormation 스택이 알림을 전송하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFORMATION_STACK_NOTIFICATION_CHECK

리소스 유형: AWS::CloudFormation::Stack

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

snsTopic1(선택 사항), 유형: 문자열

SNS 주제 ARN.

snsTopic2(선택 사항), 유형: 문자열

SNS 주제 ARN.

snsTopic3(선택 사항), 유형: 문자열

SNS 주제 ARN.

snsTopic4(선택 사항), 유형: 문자열

SNS 주제 ARN.

snsTopic5(선택 사항), 유형: 문자열

SNS 주제 ARN.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-accesslogs-enabled

표준 로깅(레거시)을 사용하여 Amazon S3 버킷에 액세스 로그를 전달하도록 Amazon Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 레거시 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_ACCESSLOGS_ENABLED

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

S3BucketName(선택 사항), 유형: 문자열

서버 액세스 로그를 저장하기 위한 Amazon S3 버킷 이름입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-associated-with-waf

Amazon CloudFront 배포가 웹 애플리케이션 방화벽(WAF) 또는 WAFv2 웹 액세스 제어 목록(ACL)과 연결되어 있는지 확인합니다. CloudFront 배포가 WAF 웹 ACL과 연결되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_ASSOCIATED_WITH_WAF

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

wafWebAclIds(선택 사항), 유형: CSV

WAF의 ACL ID 또는 WAFV2의 ACL 아마존 리소스 이름(ARN)을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-custom-ssl-certificate

Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서인지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-default-root-object-configured

Amazon CloudFront 배포가 기본 루트 객체인 특정 객체를 반환하도록 구성되어 있는지 확인합니다. Amazon CloudFront 배포에 기본 루트 객체가 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-no-deprecated-ssl-protocols

CloudFront 배포가 CloudFront 엣지 로케이션과 사용자 지정 오리진 간의 HTTPS 통신에 더 이상 사용되지 않는 SSL 프로토콜을 사용하고 있는지 확인합니다. 'OriginSslProtocols'에 'SSLv3'이 포함된 경우 이 규칙은 CloudFront 배포에 대해 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-origin-access-identity-enabled

Amazon S3 오리진 유형을 사용하는 CloudFront 배포에 원본 액세스 ID가 구성되어 있는지 확인합니다. CloudFront 배포가 S3에 의해 지원되고 모든 오리진 유형이 OAI로 구성되어 있지 않거나, 오리진이 S3 버킷이 아닌 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 오리진이 S3 버킷이 아닌 `NOT_APPLICABLE` 경우 규칙은를 반환하지 않습니다.

식별자: CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-origin-failover-enabled

오리진 그룹이 Amazon CloudFront에 대한 오리진 그룹에 있는 2개 이상의 오리진을 배포하도록 구성되어 있는지 확인합니다. 배포에 사용할 오리진 그룹이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-s3-origin-access-control-enabled

Amazon Simple Storage Service(S3) 오리진 유형을 사용하는 Amazon CloudFront 배포에 원본 액세스 제어(OAC)가 활성화되어 있는지 확인합니다. OAC가 활성화되지 않은 Amazon S3 오리진을 사용하는 CloudFront 배포의 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-s3-origin-non-existent-bucket

Amazon CloudFront 배포가 존재하지 않는 S3 버킷을 가리키는지 확인합니다. CloudFront 배포의 'S3OriginConfig'가 존재하지 않는 S3 버킷을 가리키는 경우 규칙은 NON_COMPLIANT입니다. 이 규칙은 정적 웹 사이트 호스팅을 사용하는 S3 버킷을 평가하지 않습니다.

식별자: CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

리소스 유형: AWS::CloudFront::Distribution

트리거 유형: 주기적

AWS 리전: 중국(베이징), 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-security-policy-check

Amazon CloudFront 배포가 시청자 연결에 대해 최소 보안 정책 및 TLSv1.2 이상의 암호 그룹을 사용하고 있는지 확인합니다. minimumProtocolVersion이 TLSv1.2_2018 이하이면 CloudFront 배포의 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_SECURITY_POLICY_CHECK

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-sni-enabled

Amazon CloudFront 배포가 사용자 지정 SSL 인증서를 사용하고 있으며 SNI를 사용하여 HTTPS 요청을 처리하도록 구성되어 있는지 확인합니다. 사용자 지정 SSL 인증서가 연결되어 있지만 SSL 지원 메서드가 전용 IP 주소인 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_SNI_ENABLED

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-ssl-policy-check

Amazon CloudFront 배포가 지정된 보안 정책으로 구성되어 있는지 확인합니다. CloudFront 배포가 지정한 보안 정책으로 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_SSL_POLICY_CHECK

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

securityPolicies, 유형: CSV

> 확인할 규칙에 대한 CloudFront 배포 보안 정책의 쉼표로 구분된 목록입니다. 예: "TLSv1.2_2018, TLSv1.2_2019, TLSv1.2_2021". 유효한 값 목록은 Amazon CloudFront 개발자 안내서를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-traffic-to-origin-encrypted

Amazon CloudFront 배포가 사용자 지정 오리진에 대한 트래픽을 암호화하고 있는지 확인합니다. 'OriginProtocolPolicy'가 'http-only'인 경우 또는 'OriginProtocolPolicy'가 'match-viewer'이고 'ViewerProtocolPolicy'이 'allow-all'인 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudfront-viewer-policy-https

Amazon CloudFront 배포에서 HTTPS(직접 또는 리디렉션)를 사용하는지 확인합니다. ViewerProtocolPolicy의 값이 DefaultCacheBehavior 또는 CacheBehaviors에 대해 'allow-all'로 설정되어 있으면 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDFRONT_VIEWER_POLICY_HTTPS

리소스 유형: AWS::CloudFront::Distribution

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudtrail-all-read-s3-data-event-check

AWS CloudTrail 다중 리전 추적이 활성화되어 있는지 확인하고 버킷에 대한 모든 읽기 S3 데이터 이벤트를 기록합니다. 다중 리전 추적이 현재 및 향후의 모든 S3 버킷에 대해 읽은 모든 S3 데이터 이벤트 유형을 로그하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDTRAIL_ALL_READ_S3_DATA_EVENT_CHECK

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudtrail-all-write-s3-data-event-check

AWS CloudTrail 다중 리전 추적이 활성화되어 있는지 확인하고 버킷에 대한 모든 쓰기 S3 데이터 이벤트를 기록합니다. 다중 리전 추적이 현재 및 향후의 모든 S3 버킷에 대해 쓴 모든 S3 데이터 이벤트 유형을 로그하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDTRAIL_ALL_WRITE_S3_DATA_EVENT_CHECK

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudtrail-s3-bucket-access-logging

AWS CloudTrail 로그의 S3 버킷 구성에 Amazon S3 서버 액세스 로깅이 활성화되어 있는지 확인합니다. CloudTrail 추적에 대해 최소 하나 이상의 S3 버킷에 S3 서버 액세스 로깅이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDTRAIL_S3_BUCKET_ACCESS_LOGGING

리소스 유형: AWS::CloudTrail ::Trail

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudtrail-s3-bucket-public-access-prohibited

AWS CloudTrail 로그에 대한 S3 버킷 구성이 퍼블릭 액세스를 차단하는지 확인합니다. CloudTrail 추적을 위한 S3 버킷 중 최소 하나 이상에 공개적으로 액세스할 수 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDTRAIL_S3_BUCKET_PUBLIC_ACCESS_PROHIBITED

리소스 유형: AWS::CloudTrail ::Trail

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudtrail-s3-dataevents-enabled

하나 이상의 AWS CloudTrail 추적이 모든 Amazon S3S3) 데이터 이벤트를 로깅하고 있는지 확인합니다. 추적이 있거나 S3 데이터 이벤트를 기록하는 추적이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDTRAIL_S3_DATAEVENTS_ENABLED

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

s3BucketNames(선택 사항), 유형: 문자열

데이터 이벤트 로깅을 활성화해야 하는 S3 버킷 이름을 쉼표로 구분한 목록이며, 모든 S3 버킷을 확인하는 것이 기본 동작입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudtrail-security-trail-enabled

보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT입니다.

- 글로벌 서비스 이벤트를 기록함
- 다중 리전 추적임
- 로그 파일 검증이 활성화되어 있음
- KMS 키로 암호화됨
- 읽기 및 쓰기에 대한 이벤트를 기록함
- 관리 이벤트를 기록함
- 관리 이벤트를 제외하지 않음

위에서 언급한 모든 기준을 충족하는 추적이 없는 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDTRAIL_SECURITY_TRAIL_ENABLED

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudwatch-alarm-action-check

CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 선택에 따라, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDWATCH_ALARM_ACTION_CHECK

리소스 유형: AWS::CloudWatch::Alarm

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

alarmActionRequired, 유형: 문자열, 기본값: true

경보에 작업이 한 개 이상 존재합니다.

insufficientDataActionRequired, 유형: 문자열, 기본값: true

경보가 다른 상태에서 INSUFFICIENT_DATA 상태로 전환될 때 경보에 하나 이상의 작업이 있습니다.

okActionRequired, 유형: 문자열, 기본값: false

경보가 다른 상태에서 OK 상태로 전환될 때 경보에 하나 이상의 작업이 있습니다.

action1(선택 사항), 유형: 문자열

실행할 작업을 ARN으로 지정한 것입니다.

action2(선택 사항), 유형: 문자열

실행할 작업을 ARN으로 지정한 것입니다.

action3(선택 사항), 유형: 문자열

실행할 작업을 ARN으로 지정한 것입니다.

action4(선택 사항), 유형: 문자열

실행할 작업을 ARN으로 지정한 것입니다.

action5(선택 사항), 유형: 문자열

실행할 작업을 ARN으로 지정한 것입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudwatch-alarm-action-enabled-check

Amazon CloudWatch 경보 작업이 활성화된 상태인지 확인합니다. CloudWatch 경보 작업이 활성화된 상태가 아닌 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

리소스 유형: AWS::CloudWatch::Alarm

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudwatch-alarm-resource-check

리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

식별자: CLOUDWATCH_ALARM_RESOURCE_CHECK

리소스 유형: AWS::EC2::Instance, AWS::RDS::DBCluster, AWS::S3::Bucket, AWS::EC2::Volume

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

resourceType, 유형: 문자열

AWS 리소스 유형. 값은 AWS::EC2::Volume, AWS::EC2::Instance, AWS::RDS::DBCluster 또는 AWS::S3::Bucket 중 하나일 수 있습니다.

metricName, 유형: 문자열

해당 경보와 연결되어 있는 지표의 이름입니다(예: EC2 인스턴스의 경우 'CPUUtilization').

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudwatch-alarm-settings-check

지정된 지표 이름의 CloudWatch 경보 설정이 지정한 설정과 일치하는지 확인합니다.

식별자: CLOUDWATCH_ALARM_SETTINGS_CHECK

리소스 유형: AWS::CloudWatch::Alarm

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

metricName, 유형: 문자열

경보와 연결되어 있는 지표의 이름입니다.

threshold(선택 사항), 유형: int

지정한 통계를 비교할 때 기준으로 삼는 값입니다.

evaluationPeriods(선택 사항), 유형: int

지정 임계값에 대한 데이터 비교가 이루어지는 기간의 일수입니다.

period(선택 사항), 유형: int, 기본값: 300

지정한 통계가 적용되는 기간을 초로 나타낸 것입니다.

comparisonOperator(선택 사항), 유형: 문자열

지정한 통계와 임계값을 비교할 때 사용하는 작업입니다(예: 'GreaterThanThreshold').

statistic(선택 사항), 유형: 문자열

경보와 연결되어 있는 지표의 통계(예: 'Average' 또는 'Sum')입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudwatch-log-group-encrypted

Amazon CloudWatch 로그 그룹이 AWS KMS 키 또는 지정된 AWS KMS 키 ID로 암호화되었는지 확인합니다. CloudWatch 로그 그룹이 KMS 키로 암호화되지 않았거나, 규칙 파라미터에 제공되지 않은 KMS 키로 암호화된 경우 규칙은 NON_COMPLIANT입니다.

식별자: CLOUDWATCH_LOG_GROUP_ENCRYPTED

리소스 유형: AWS::Logs::LogGroup

트리거 유형: 주기적

AWS 리전: 중동(UAE), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

KmsKeyId(선택 사항), 유형: 문자열

로그 그룹을 암호화하는 데 사용되는 KMS 키에 대한 ID의 Amazon 리소스 이름(ARN)입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloud-trail-cloud-watch-logs-enabled

AWS CloudTrail 추적이 CloudWatch 로그로 로그를 전송하도록 구성되어 있는지 확인합니다. 추적의 CloudWatchLogsLogGroupArn 속성이 비어 있을 경우 추적은 NON_COMPLIANT입니다.

식별자: CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

리소스 유형: AWS::CloudTrail ::Trail

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

expectedDeliveryWindowAge(선택 사항), 유형: int

규정 준수를 충족하는 가장 최신 CloudWatch 로그 전송의 최대 보존 기간(시간)입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloudtrail-enabled

> **Important**
>
> 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다.

AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

식별자: CLOUD_TRAIL_ENABLED

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

s3BucketName(선택 사항), 유형: 문자열

CloudTrail이 로그 파일을 전달할 S3 버킷의 이름입니다.

snsTopicArn(선택 사항), 유형: 문자열

CloudTrail이 알림에 사용할 SNS 주제 ARN입니다.

cloudWatchLogsLogGroupArn(선택 사항), 유형: 문자열

CloudTrail이 데이터를 전송할 CloudWatch 로그 그룹 ARN입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloud-trail-encryption-enabled

가 서버 측 암호화(SSE) AWS Key Management Service (AWS KMS) 암호화를 사용하도록 AWS CloudTrail 구성되어 있는지 확인합니다. KmsKeyId가 정의되어 있으면 규칙은 COMPLIANT입니다.

식별자: CLOUD_TRAIL_ENCRYPTION_ENABLED

리소스 유형: AWS::CloudTrail ::Trail

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cloud-trail-log-file-validation-enabled

AWS CloudTrail이 모든 추적에서 파일 검증을 활성화해야 한다고 log. AWS recommds와 함께 서명된 다이제스트 파일을 생성하는지 확인합니다. 유효성 검사가 활성화되지 않은 경우 규칙은 NON_COMPLIANT로 간주됩니다.

식별자: CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

리소스 유형: AWS::CloudTrail ::Trail

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cmk-backing-key-rotation-enabled

각 키에 대해 자동 키 교체가 활성화되어 있는지 확인하고 고객이 생성한 AWS KMS 키의 키 ID와 일치합니다. 리소스의 AWS Config 레코더 역할에 kms:DescribeKey 권한이 없는 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 비대칭 KMS 키, HMAC KMS 키, 가져온 키 구성 요소가 있는 KMS 키, 사용자 지정 키 스토어의 KMS 키에서는 자동 키 교체가 지원되지 않습니다.

식별자: CMK_BACKING_KEY_ROTATION_ENABLED

리소스 유형: AWS::KMS::Key

트리거 유형: 주기적

AWS 리전: 중동(UAE) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codebuild-project-artifact-encryption

AWS CodeBuild 프로젝트에 모든 아티팩트에 대한 암호화가 활성화되어 있는지 확인합니다. 기본 또는 보조(있는 경우) 아티팩트 구성에 대해 'encryptionDisabled'가 'true'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION

리소스 유형: AWS::CodeBuild::Project

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codebuild-project-environment-privileged-check

AWS CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있는지 확인합니다. 'privilegedMode'가 'true'로 설정된 경우 CodeBuild 프로젝트의 규칙은 NON_COMPLIANT입니다.

식별자: CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

리소스 유형: AWS::CodeBuild::Project

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

exemptedProjects(선택 사항), 유형: CSV

> 값이 'true'인 'privilegedMode'를 사용할 수 있는 CodeBuild 프로젝트 이름을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codebuild-project-envvar-awscred-check

프로젝트에 환경 변수 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 포함되어 있는지 확인합니다. 프로젝트 환경 변수에 일반 텍스트 자격 증명이 포함된 경우, 이 규칙은 NON_COMPLIANT로 간주됩니다.

식별자: CODEBUILD_PROJECT_ENVVAR_AWSCRED_CHECK

리소스 유형: AWS::CodeBuild::Project

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(말레이시아), 멕시코(중부), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codebuild-project-logging-enabled

AWS CodeBuild 프로젝트 환경에 하나 이상의 로그 옵션이 활성화되어 있는지 확인합니다. 모든 현재 로그 구성의 상태가 'DISABLED'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: CODEBUILD_PROJECT_LOGGING_ENABLED

리소스 유형: AWS::CodeBuild::Project

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

s3BucketNames(선택 사항), 유형: 문자열

S3 로그가 구성된 경우 로그를 전송해야 하는 Amazon S3 버킷 이름을 쉼표로 구분한 목록입니다.

cloudWatchGroupNames(선택 사항), 유형: 문자열

CloudWatch 로그가 구성된 경우 로그를 전송해야 하는 Amazon CloudWatch 로그 그룹 이름을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codebuild-project-s3-logs-encrypted

Amazon S3 Logs로 구성된 a AWS CodeBuild 프로젝트에 로그에 암호화가 활성화되어 있는지 확인합니다. CodeBuild 프로젝트의 S3LogsConfig에서 'encryptionDisabled'가 'true'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

리소스 유형: AWS::CodeBuild::Project

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

exemptedProjects(선택 사항), 유형: CSV

암호화되지 않은 로그를 출력할 수 있는 CodeBuild 프로젝트 이름을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codebuild-project-source-repo-url-check

Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함되어 있는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.

식별자: CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

리소스 유형: AWS::CodeBuild::Project

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(말레이시아), 멕시코(중부), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codebuild-report-group-encrypted-at-rest

AWS CodeBuild 보고서 그룹에 저장 시 암호화 설정이 활성화되어 있는지 확인합니다. 'EncryptionDisabled'가 'true'인 경우 규칙은 NON_COMPLIANT입니다.

식별자: CODEBUILD_REPORT_GROUP_ENCRYPTED_AT_REST

리소스 유형: AWS::CodeBuild::ReportGroup

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codedeploy-auto-rollback-monitor-enabled

배포 그룹이 자동 배포 롤백 및 경보가 첨부된 배포 모니터링으로 구성되어 있는지 확인합니다. AutoRollbackConfiguration 또는 AlarmConfiguration이 구성되지 않았거나 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED

리소스 유형: AWS::CodeDeploy::DeploymentGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codedeploy-deployment-group-auto-rollback-enabled

AWS CodeDeploy 배포 그룹에 자동 롤백 구성이 활성화되어 있는지 확인합니다. configuration.autoRollbackConfiguration.enabled가 false이거나 존재하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: CODEDEPLOY_DEPLOYMENT_GROUP_AUTO_ROLLBACK_ENABLED

리소스 유형: AWS::CodeDeploy::DeploymentGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codedeploy-deployment-group-outdated-instances-update

AWS CodeDeploy 배포 그룹이 오래된 인스턴스를 자동으로 업데이트하는지 확인합니다. configuration.outdatedInstancesStrategy가 'IGNORE'인 경우 규칙은 NON_COMPLIANT입니다.

식별자: CODEDEPLOY_DEPLOYMENT_GROUP_OUTDATED_INSTANCES_UPDATE

리소스 유형: AWS::CodeDeploy::DeploymentGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codedeploy-ec2-minimum-healthy-hosts-configured

EC2/온프레미스 Compute Platform의 배포 그룹이 최소 정상 호스트 플릿 비율 또는 호스트 수가 입력 임계값보다 크거나 같게 구성되어 있는지 확인합니다. 둘 중 하나라도 임계값 미만인 경우 규칙은 NON_COMPLIANT입니다.

식별자: CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED

리소스 유형: AWS::CodeDeploy::DeploymentGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

minimumHealthyHostsFleetPercent(선택 사항), 유형: int, 기본값: 66

배포 중 정상 호스트 플릿의 최소 비율입니다. 기본값은 66%입니다.

minimumHealthyHostsHostCount(선택 사항), 유형: int, 기본값: 1

배포 중 플릿에 있는 정상 호스트의 최소 비율입니다. 기본값은 1로 설정됩니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codedeploy-lambda-allatonce-traffic-shift-disabled

Lambda Compute Platform의 배포 그룹이 기본 배포 구성을 사용하지 않는지 확인합니다. 배포 그룹이 배포 구성 'CodeDeployDefault.LambdaAllAtOnce'를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

식별자: CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

리소스 유형: AWS::CodeDeploy::DeploymentGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codeguruprofiler-profiling-group-tagged

Amazon CodeGuru Profiler 프로파일링 그룹에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: CODEGURUPROFILER_PROFILING_GROUP_TAGGED

리소스 유형: AWS::CodeGuruProfiler::ProfilingGroup

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codegurureviewer-repository-association-tagged

Amazon CodeGuru Reviewer 리포지토리 연결에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: CODEGURUREVIEWER_REPOSITORY_ASSOCIATION_TAGGED

리소스 유형: AWS::CodeGuruReviewer::RepositoryAssociation

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codepipeline-deployment-count-check

AWS CodePipeline의 첫 번째 배포 단계가 둘 이상의 배포를 수행하는지 확인합니다. 또는 각각의 이후 단계에서 지정된 배포 횟수(`deploymentLimit`) 이상을 배포하는지 확인합니다.

식별자: CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

리소스 유형: AWS::CodePipeline::Pipeline

트리거 0유형: 구성 변경

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

deploymentLimit(선택 사항), 유형: int

각 단계에서 수행할 수 있는 배포 최대 횟수입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

codepipeline-region-fanout-check

AWS CodePipeline의 각 단계가 이전의 모든 결합된 단계에서 AWS CodePipeline한 리전 수의 N배 이상으로 배포되는지 확인합니다. 여기서 N은 리전 팬아웃 번호입니다. 첫 번째 배포 단계에서는 최대 한 리전에 배포할 수 있으며, 두 번째 배포 단계에서는 `regionFanoutFactor`에 지정된 최대 수로 배포할 수 있습니다. `regionFanoutFactor`를 제공하지 않을 경우 기본값은 3입니다. 예를 들어 첫 번째 배포 단계에서 한 리전에 배포하고 두 번째 구축 단계에서 3개 리전에 배포하는 경우, 세 번째 배포 단계에서는 12개 리전, 즉 이전 단계에 리전 팬아웃(3)을 곱한 수의 리전에 배포할 수 있습니다. 첫 단계에서 배포가 두 개 이상 리전에 배포하거나, 두 번째 단계에서 세 개 이상의 리전에 배포하거나, 세 번째 단계에서 12개 이상의 리전에 배포할 경우 규칙이 NON_COMPLIANT로 간주됩니다.

식별자: CODEPIPELINE_REGION_FANOUT_CHECK

리소스 유형: AWS::CodePipeline::Pipeline

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 중동(UAE), 유럽(프랑크푸르트), 남아메리카(상파울루), 아시아 태평양(하이데라바드), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 이스라엘(텔아비브), 캐나다(중부) 리전에서만 사용 가능

파라미터:

regionFanoutFactor(선택 사항), 유형: int, 기본값: 3

모든 이전 단계에서 AWS CodePipeline이 배포한 리전 수는 모든 스테이지가 배포할 수 있는 허용 가능한 리전 수입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cognito-identity-pool-unauth-access-check

Amazon Cognito 자격 증명 풀이 인증되지 않은 자격 증명을 허용하는지 확인합니다. 자격 증명 풀이 인증되지 않은 자격 증명을 허용하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

식별자: COGNITO_IDENTITY_POOL_UNAUTH_ACCESS_CHECK

리소스 유형: AWS::Cognito::IdentityPool

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(서울), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cognito-user-pool-advanced-security-enabled

Amazon Cognito 사용자 풀에 표준 인증을 위한 고급 보안이 활성화되어 있는지 확인합니다. 고급 보안이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다. 선택적으로 확인할 규칙에 대한 고급 보안 모드를 지정할 수 있습니다.

식별자: COGNITO_USER_POOL_ADVANCED_SECURITY_ENABLED

리소스 유형: AWS::Cognito::UserPool

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(홍콩), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

SecurityMode(선택 사항), 유형: 문자열

> 확인할 규칙에 대한 고급 보안 모드의 문자열 값입니다. 제공된 경우 사용자 풀의 고급 보안 모드가이 파라미터 값과 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다. 유효한 값은 AUDIT 및 ENFORCED입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cognito-user-pool-tagged

Amazon Cognito 사용자 풀에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: COGNITO_USER_POOL_TAGGED

리소스 유형: AWS::Cognito::UserPool

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

connect-instance-logging-enabled

Amazon CloudWatch 로그 그룹에서 Amazon Connect 인스턴스에 흐름 로그가 활성화되어 있는지 확인합니다. Amazon CloudWatch Amazon Connect 인스턴스에 흐름 로그가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: CONNECT_INSTANCE_LOGGING_ENABLED

리소스 유형: AWS::Connect::Instance

트리거 0유형: 구성 변경

AWS 리전: 아프리카(케이프타운), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

customerprofiles-object-type-allow-profile-creation

Amazon Connect Customer Profiles 객체 유형이 없는 경우 새 표준 프로필 생성을 허용하는지 확인합니다. configuration.AllowProfileCreation이 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: CUSTOMERPROFILES_OBJECT_TYPE_ALLOW_PROFILE_CREATION

리소스 유형: AWS::CustomerProfiles::ObjectType

트리거 0유형: 구성 변경

AWS 리전: 아프리카(케이프타운), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

customerprofiles-object-type-tagged

Amazon Connect Customer Profiles 객체 유형에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: CUSTOMERPROFILES_OBJECT_TYPE_TAGGED

리소스 유형: AWS::CustomerProfiles::ObjectType

트리거 0유형: 구성 변경

AWS 리전: 아프리카(케이프타운), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

custom-eventbus-policy-attached

Amazon EventBridge 사용자 지정 이벤트 버스에 리소스 기반 정책이 연결되어 있는지 확인합니다. 사용자 지정 이벤트 버스 정책에 연결된 리소스 기반 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: CUSTOM_EVENTBUS_POLICY_ATTACHED

리소스 유형: AWS::Events::EventBus

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

custom-schema-registry-policy-attached

사용자 지정 Amazon EventBridge 스키마 레지스트리에 리소스 정책이 연결되어 있는지 확인합니다. 리소스 정책이 연결되지 않은 사용자 지정 스키마 레지스트리의 경우 규칙은 NON_COMPLIANT입니다.

식별자: CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

리소스 유형: AWS::EventSchemas::Registry

트리거 유형: 주기적

AWS 리전: 유럽(스톡홀름), 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 아시아 태평양(홍콩), 미국 동부(버지니아 북부), 아시아 태

평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

cw-loggroup-retention-period-check

Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 `MinRetentionTime`보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.

> **Note**
> 로그 그룹의 보존 설정이 '만기 없음'인 경우 규칙은 COMPLIANT로 표시됩니다.

식별자: CW_LOGGROUP_RETENTION_PERIOD_CHECK

리소스 유형: AWS::Logs::LogGroup

트리거 유형: 주기적

AWS 리전: 중동(UAE) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

LogGroupNames(선택 사항), 유형: CSV

보존 기간을 확인하기 위한 로그 그룹 이름을 쉼표로 구분한 목록입니다.

MinRetentionTime(선택 사항), 유형: int

보존일 수를 지정합니다. 유효한 값은 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, 3653입니다. 기본 보존 기간은 365일입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

datasync-task-data-verification-enabled

전송이 끝날 때 추가 확인을 수행할 수 있도록 AWS DataSync 작업에 데이터 확인이 활성화되어 있는지 확인합니다. configuration.Options.VerifyMode가 'NONE'인 경우 규칙은 NON_COMPLIANT입니다.

식별자: DATASYNC_TASK_DATA_VERIFICATION_ENABLED

리소스 유형: AWS::DataSync::Task

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

datasync-task-logging-enabled

AWS DataSync 태스크에 Amazon CloudWatch 로깅이 활성화되어 있는지 확인합니다. AWS DataSync 태스크에 Amazon CloudWatch 로깅이 활성화되어 있지 않거나 로깅 수준이 지정한 로깅 수준과 동일하지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DATASYNC_TASK_LOGGING_ENABLED

리소스 유형: AWS::DataSync::Task

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

logLevel(선택 사항), 유형: 문자열

로깅 수준의 문자열 값입니다. 유효한 값에는 'BASIC' 및 'TRANSFER'가 포함됩니다. 지정하지 않은 경우 기본값은 'BASIC'입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

datasync-task-tagged

AWS DataSync 작업에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: DATASYNC_TASK_TAGGED

리소스 유형: AWS::DataSync::Task

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dax-encryption-enabled

Amazon DynamoDB Accelerator(DAX) 클러스터가 암호화되어 있는지 확인합니다. DAX 클러스터가 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DAX_ENCRYPTION_ENABLED

리소스 유형: AWS::DAX::Cluster

트리거 유형: 주기적

AWS 리전: 유럽(스톡홀름), 중국(베이징), 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 유럽(스페인), 중국(닝샤) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dax-tls-endpoint-encryption

Amazon DynamoDB Accelerator(DAX) 클러스터에 ClusterEndpointEncryptionType이 TLS로 설정되어 있는지 확인합니다. DAX 클러스터가 Transport Layer Security(TLS)로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DAX_TLS_ENDPOINT_ENCRYPTION

리소스 유형: AWS::DAX::Cluster

트리거 유형: 주기적

AWS 리전: 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능합니다.

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

db-instance-backup-enabled

RDS DB 인스턴스에 백업이 활성화되어 있는지 확인합니다. 이 규칙은 필요에 따라 백업 보존 기간과 백업 기간을 확인합니다.

식별자: DB_INSTANCE_BACKUP_ENABLED

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

backupRetentionPeriod(선택 사항), 유형: int

백업의 보존 기간입니다.

backupRetentionMinimum(선택 사항), 유형: int

백업의 최소 보존 기간입니다.

preferredBackupWindow(선택 사항), 유형: 문자열

백업 생성의 시간 범위입니다.

checkReadReplicas(선택 사항), 유형: boolean

RDS DB 인스턴스에 읽기 전용 복제본 백업이 활성화되어 있는지 확인합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

desired-instance-tenancy

EC2 인스턴스의 '테넌시' 값을 확인합니다. AMI ID가 해당 AMI에서 시작되도록 지정되었는지 또는 호스트 ID가 해당 전용 호스트에서 시작되었는지도 확인합니다. 인스턴스가 목록에 있는 호스트 및 AMI(지정된 경우)와 일치하면 규칙은 COMPLIANT입니다.

식별자: DESIRED_INSTANCE_TENANCY

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

테넌시, 유형: 문자열

원하는 인스턴스의 테넌시입니다. 유효한 값은 DEDICATED, HOST, DEFAULT입니다.

imageId(선택 사항), 유형: CSV

이 규칙은 지정된 ID가 있는 AMI에서 시작된 인스턴스만 평가합니다. AMI ID가 여러 개인 경우 쉼표로 구분합니다.

hostId(선택 사항), 유형: CSV

인스턴스를 시작할 EC2 전용 호스트의 ID입니다. 호스트 ID가 여러 개인 경우 쉼표로 구분합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

desired-instance-type

EC2 인스턴스가 특정 인스턴스 유형에 해당하는지 확인합니다. 파라미터 목록에 EC2 인스턴스가 지정되지 않은 경우 규칙은 NON_COMPLIANT입니다. 지원되는 EC2 인스턴스 유형 목록은 Linux 인스턴스용 EC2 사용자 설명서의 인스턴스 유형을 참조하세요.

식별자: DESIRED_INSTANCE_TYPE

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

instanceType, 유형: CSV

EC2 인스턴스 유형을 쉼표로 구분하여 기입한 목록(예: "t2.small, m4.large, i2.xlarge")입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dms-auto-minor-version-upgrade-check

AWS Database Migration Service(AWS DMS) 복제 인스턴스에 자동 마이너 버전 업그레이드가 활성화되어 있는지 확인합니다. AWS DMS 복제 인스턴스가 자동 마이너 버전 업그레이드로 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

리소스 유형: AWS::DMS::ReplicationInstance

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dms-endpoint-ssl-configured

AWS Database Migration Service(AWS DMS) 엔드포인트가 SSL 연결로 구성되어 있는지 확인합니다. AWS DMS에 SSL 연결이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

컨텍스트: SSL/TLS 연결이 클라이언트와 DB 인스턴스 사이에 전송되는 데이터를 암호화하여 하나의 보안 계층을 제공합니다. 서버 인증서를 사용하면 연결이 Amazon RDS DB 인스턴스클러스터에 연결

되고 있는지 검증하는 추가 보안 계층을 제공할 수 있습니다. 이 보안 계층에서는 사용자가 프로비저닝한 모든 DB 인스턴스에 자동으로 설치되는 서버 인증서를 확인하는 방법으로 검증을 수행합니다. 에서 SSL 연결을 활성화하면 마이그레이션 중에 데이터의 기밀성을 AWS DMS보호할 수 있습니다.

에 대한 SSL 연결을 구성하려면 Amazon Relational Database Service 사용 설명서의 SSL/TLS를 사용하여 DB 인스턴스 또는 클러스터에 대한 연결 암호화를 AWS DMS참조하세요.

식별자: DMS_ENDPOINT_SSL_CONFIGURED

리소스 유형: AWS::DMS::Endpoint

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dms-endpoint-tagged

AWS DMS 엔드포인트에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: DMS_ENDPOINT_TAGGED

리소스 유형: AWS::DMS::Endpoint

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS

GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dms-mongo-db-authentication-enabled

MongoDb 데이터 스토어의 AWS 데이터베이스 마이그레이션 서비스(AWS DMS) 엔드포인트가 암호 기반 인증 및 액세스 제어를 위해 활성화되어 있는지 확인합니다. 암호 기반 인증 및 액세스 제어가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DMS_MONGO_DB_AUTHENTICATION_ENABLED

리소스 유형: AWS::DMS::Endpoint

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dms-neptune-iam-authorization-enabled

Amazon Neptune AWS 데이터베이스의 Database Migration Service(AWS DMS) 엔드포인트가 IAM 권한 부여로 구성되어 있는지 확인합니다. Neptune이 대상인 AWS DMS 엔드포인트에 IamAuthEnabled가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: DMS_NEPTUNE_IAM_AUTHORIZATION_ENABLED

리소스 유형: AWS::DMS::Endpoint

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dms-redis-tls-enabled

Redis 데이터 스토어의 AWS Database Migration Service(AWS DMS) 엔드포인트가 다른 엔드포인트와 통신하는 데이터의 TLS/SSL 암호화에 대해 활성화되어 있는지 확인합니다. TLS/SSL 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DMS_REDIS_TLS_ENABLED

리소스 유형: AWS::DMS::Endpoint

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비

브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dms-replication-not-public

AWS Database Migration Service(AWS DMS) 복제 인스턴스가 퍼블릭인지 확인합니다. PubliclyAccessible 필드가 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: DMS_REPLICATION_NOT_PUBLIC

리소스 유형: AWS::DMS::ReplicationInstance

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dms-replication-task-sourcedb-logging

소스 데이터베이스의 AWS DMS 복제 작업에 대해 유효한 심각도 수준으로 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않았거나, 소스 데이터베이스의 DMS 복제 태스크에 대한 로그의 심각도 수준이 유효하지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DMS_REPLICATION_TASK_SOURCEDB_LOGGING

리소스 유형: AWS::DMS::ReplicationTask

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dms-replication-task-tagged

AWS DMS 복제 작업에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: DMS_REPLICATION_TASK_TAGGED

리소스 유형: AWS::DMS::ReplicationTask

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dms-replication-task-targetdb-logging

대상 데이터베이스의 AWS DMS 복제 작업 이벤트에 대해 유효한 심각도 수준으로 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않았거나, 대상 데이터베이스의 복제 태스크에 대한 로그의 심각도 수준이 유효하지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DMS_REPLICATION_TASK_TARGETDB_LOGGING

리소스 유형: AWS::DMS::ReplicationTask

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

docdb-cluster-audit-logging-enabled

Amazon DocumentDB(MongoDB 호환) 인스턴스 클러스터에서 CloudWatch 로그 내보내기가 감사 로그에 대해 활성화되어 있는지 확인합니다. Amazon DocumentDB 인스턴스 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DOCDB_CLUSTER_AUDIT_LOGGING_ENABLED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 미국 서부(캘리포니아 북부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

docdb-cluster-backup-retention-check

Amazon Document DB 클러스터 보존 기간이 특정 일수로 설정되어 있는지 확인합니다. 보존 기간이 파라미터에서 지정된 값보다 짧은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DOCDB_CLUSTER_BACKUP_RETENTION_CHECK

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 미국 서부(캘리포니아 북부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

minimumBackupRetentionPeriod(선택 사항), 유형: int

> 백업을 보관해야 할 최소 기간(일)입니다. 유효한 값은 1~35이며, 기본값은 7입니다. 값이 'backupRetentionPeriod'보다 큰 경우 이 규칙은 NON_COMPLIANT입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

docdb-cluster-deletion-protection-enabled

Amazon DocumentDB(MongoDB 호환) 클러스터에 삭제 방지가 활성화되어 있는지 확인합니다. Amazon DocumentDB 클러스터의 삭제 방지 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: DOCDB_CLUSTER_DELETION_PROTECTION_ENABLED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 미국 서부(캘리포니아 북부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

docdb-cluster-encrypted

Amazon DocumentDB(MongoDB 호환) 클러스터에 대해 스토리지 암호화가 활성화되어 있는지 확인합니다. 스토리지 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DOCDB_CLUSTER_ENCRYPTED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 미국 서부(캘리포니아 북부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: CSV

암호화된 클러스터의 KmsKeyID와 비교할 수 있는 KMS 키 ARN을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

docdb-cluster-encrypted-in-transit

Amazon DocumentDB 클러스터에 대한 연결이 전송 중 암호화를 사용하도록 구성되어 있는지 확인합니다. 파라미터 그룹이 "in-sync"가 아니거나 TLS 파라미터가 "disabled" 또는의 값으로 설정된 경우 규칙은 NON_COMPLIANT입니다`excludeTlsParameters`.

식별자: DOCDB_CLUSTER_ENCRYPTED_IN_TRANSIT

리소스 유형: AWS::RDS::DBCluster

트리거 유형: 주기적

AWS 리전: 유럽(스톡홀름), 중동(바레인), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 미국 서부(캘리포니아 북부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

excludeTlsParameters(선택 사항), 유형: CSV

확인할 규칙에 대한 TLS 클러스터 파라미터의 쉼표로 구분된 목록입니다. 기본값: '비활성화됨'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

docdb-cluster-snapshot-public-prohibited

Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인지 확인합니다. Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

식별자: DOCDB_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

리소스 유형: AWS::RDS::DBClusterSnapshot

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 중동(UAE), 유럽(프랑크푸르트), 남아메리카(상파울루), 아시아 태평양(홍콩), 아시아 태평양(하이데라바드), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 유럽(밀라노), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dynamodb-autoscaling-enabled

Amazon DynamoDB 테이블 또는 글로벌 보조 인덱스가 오토 스케일링이 활성화된 온디맨드 모드 또는 프로비저닝된 모드를 사용하여 읽기/쓰기 용량을 처리할 수 있는지 확인합니다. 오토 스케일링이 활성화되지 않은 상태에서 두 가지 모드 중 하나를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

식별자: DYNAMODB_AUTOSCALING_ENABLED

리소스 유형: AWS::DynamoDB::Table

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

minProvisionedReadCapacity(선택 사항), 유형: int

오토 스케일링 그룹에 할당해야 하는 읽기 용량의 최소 단위 수입니다.

maxProvisionedReadCapacity(선택 사항), 유형: int

오토 스케일링 그룹에 할당해야 하는 읽기 용량의 최대 단위 수입니다.

targetReadUtilization(선택 사항), 유형: Double

읽기 용량의 목표 사용률(%)입니다. 목표 사용률이란 할당된 용량 대 사용한 용량의 비율로 나타낸 값입니다.

minProvisionedWriteCapacity(선택 사항), 유형: int

오토 스케일링 그룹에 할당해야 하는 쓰기 용량의 최소 단위 수입니다.

maxProvisionedWriteCapacity(선택 사항), 유형: int

오토 스케일링 그룹에 할당해야 하는 쓰기 용량의 최대 단위 수입니다.

targetWriteUtilization(선택 사항), 유형: Double

쓰기 용량의 목표 사용률(%)입니다. 목표 사용률이란 할당된 용량 대 사용한 용량의 비율로 나타낸 값입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dynamodb-in-backup-plan

Amazon DynamoDB 테이블이 AWS 백업 계획에 있는지 확인합니다. Amazon DynamoDB 테이블이 AWS 백업 계획에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: DYNAMODB_IN_BACKUP_PLAN

리소스 유형: AWS::DynamoDB::Table

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dynamodb-last-backup-recovery-point-created

지정된 기간 내에 Amazon DynamoDB 테이블에 대한 복구 시점이 생성되었는지 확인합니다. 지정된 기간 내에 생성된 해당하는 복구 시점이 DynamoDB 테이블 볼륨에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED

리소스 유형: AWS::DynamoDB::Table

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 DynamoDB 테이블의 태그입니다(JSON 형식 `{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 DynamoDB 테이블의 이름입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 744시간, 일수는 31일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dynamodb-meets-restore-time-target

Amazon DynamoDB 테이블의 복원 시간이 지정된 기간을 충족하는지 확인합니다. Amazon DynamoDB 테이블의 LatestRestoreExecutionTimeMinutes가 maxRestoreTime(분)보다 큰 경우 규칙은 NON_COMPLIANT입니다.

식별자: DYNAMODB_MEETS_RESTORE_TIME_TARGET

리소스 유형: AWS::DynamoDB::Table

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

maxRestoreTime, 유형: int

허용되는 최대 복원 런타임의 숫자 값입니다.

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 DynamoDB 테이블의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 DynamoDB 테이블의 이름입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dynamodb-pitr-enabled

Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: DYNAMODB_PITR_ENABLED

리소스 유형: AWS::DynamoDB::Table

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dynamodb-resources-protected-by-backup-plan

Amazon DynamoDB 테이블이 백업 계획에 의해 보호되는지 확인합니다. DynamoDB 테이블을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

리소스 유형: AWS::DynamoDB::Table

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 DynamoDB 테이블의 태그입니다(JSON 형식 `{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 DynamoDB 테이블의 이름입니다.

crossRegionList(선택 사항), 유형: 문자열

리전 간 백업 사본을 보관할 대상 리전을 쉼표로 구분한 목록입니다.

crossAccountList(선택 사항), 유형: 문자열

계정 간 백업 사본을 보관할 대상 계정을 쉼표로 구분한 목록입니다.

maxRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최대 보존 기간(일)

minRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최소 보존 기간(일)

backupVaultLockCheck(선택 사항), 유형: 문자열

허용되는 값: 'True' 또는 'False'. 리소스가 잠긴 볼트에 백업되어 있는지 확인하는 규칙에 'True'를 입력합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dynamodb-table-deletion-protection-enabled

Amazon DynamoDB 테이블에 삭제 방지가 활성화 상태로 설정되어 있는지 확인합니다. 테이블에 삭제 방지 기능이 비활성화 상태로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

리소스 유형: AWS::DynamoDB::Table

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dynamodb-table-encrypted-kms

Amazon DynamoDB 테이블이 AWS Key Management Service(KMS)로 암호화되어 있는지 확인합니다. Amazon DynamoDB 테이블이 AWS KMS로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다. 암호화된 AWS KMS 키가 `kmsKeyArns` 입력 파라미터에 없는 경우에도 규칙은 NON_COMPLIANT입니다.

식별자: DYNAMODB_TABLE_ENCRYPTED_KMS

리소스 유형: AWS::DynamoDB::Table

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: CSV

> Amazon DynamoDB 테이블을 암호화하는 데 허용되는 AWS KMS 키 ARNs의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dynamodb-table-encryption-enabled

Amazon DynamoDB 테이블이 암호화되어 있는지 확인하고 상태를 확인합니다. 상태가 활성화되었거나 활성화 중인 경우 규칙이 COMPLIANT로 간주됩니다.

식별자: DYNAMODB_TABLE_ENCRYPTION_ENABLED

리소스 유형: AWS::DynamoDB::Table

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 중동(바레인), 아시아 태평양(자카르타), 아프리카(케이프타운), 아시아 태평양(홍콩), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 유럽(밀라노), 유럽(스페인), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

dynamodb-throughput-limit-check

프로비저닝된 DynamoDB 처리량이 계정의 최대 한도에 근접하고 있는지 확인합니다. 기본적으로 이 규칙은 프로비저닝된 처리량이 계정 한도의 80%를 초과하는지 확인합니다.

식별자: DYNAMODB_THROUGHPUT_LIMIT_CHECK

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

accountRCUThresholdPercentage(선택 사항), 유형: int, 기본값: 80

계정에 프로비저닝된 읽기 용량 단위의 백분율입니다. 이 값에 도달하면 규칙이 noncompliant로 표시됩니다.

accountWCUThresholdPercentage(선택 사항), 유형: int, 기본값: 80

계정에 프로비저닝된 쓰기 용량 단위의 백분율입니다. 이 값에 도달하면 규칙이 noncompliant로 표시됩니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ebs-in-backup-plan

AWS 백업의 백업 계획에 Amazon Elastic Block Store(Amazon EBS) 볼륨이 추가되었는지 확인합니다. Amazon EBS 볼륨이 백업 계획에 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: EBS_IN_BACKUP_PLAN

리소스 유형: AWS::EC2::Volume

트리거 유형: 주기적

AWS 리전: 아시아 태평양(멜버른), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ebs-last-backup-recovery-point-created

Amazon Elastic Block Store(Amazon EBS)에 대한 복구 시점이 생성되었는지 확인합니다. 지정된 기간 내에 생성된 해당하는 복구 시점이 Amazon EBS 볼륨에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EBS_LAST_BACKUP_RECOVERY_POINT_CREATED

리소스 유형: AWS::EC2::Volume

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EBS 볼륨의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EBS 볼륨의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 744시간, 일수는 31일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ebs-meets-restore-time-target

Amazon Elastic Block Store(Amazon EBS)의 복원 시간이 지정된 기간을 충족하는지 확인합니다. Amazon EBS 볼륨의 LatestRestoreExecutionTimeMinutes가 maxRestoreTime(분)보다 큰 경우 규칙은 NON_COMPLIANT입니다.

식별자: EBS_MEETS_RESTORE_TIME_TARGET

리소스 유형: AWS::EC2::Volume

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

maxRestoreTime, 유형: int

허용되는 최대 복원 런타임의 숫자 값입니다.

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EBS 볼륨의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EBS 볼륨의 ID입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ebs-optimized-instance

Amazon EBS 최적화가 가능한 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 대해 Amazon EBS 최적화가 활성화되어 있는지 확인합니다. EBS 최적화가 가능한 Amazon EC2 인스턴스에 대해 EBS 최적화가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> EBS 최적화된 EC2 인스턴스는 기본적으로 항상 규칙 평가 시 `COMPLIANT`를 반환합니다.

식별자: EBS_OPTIMIZED_INSTANCE

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ebs-resources-in-logically-air-gapped-vault

Amazon Elastic Block Store(Amazon EBS) 볼륨이 논리적 에어 갭 저장소에 있는지 확인합니다. Amazon EBS 볼륨이 지정된 기간 내에 논리적 에어 갭 저장소에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EBS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

리소스 유형: AWS::EC2::Volume

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EBS 볼륨의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EBS 볼륨의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 2184시간, 일수는 91일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ebs-resources-protected-by-backup-plan

Amazon Elastic Block Store(Amazon EBS) 볼륨이 백업 계획에 의해 보호되는지 확인합니다. Amazon EBS 볼륨을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

리소스 유형: AWS::EC2::Volume

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EBS 볼륨의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EBS 볼륨의 ID입니다.

crossRegionList(선택 사항), 유형: 문자열

리전 간 백업 사본을 보관할 대상 리전을 쉼표로 구분한 목록입니다.

crossAccountList(선택 사항), 유형: 문자열

계정 간 백업 사본을 보관할 대상 계정을 쉼표로 구분한 목록입니다.

maxRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최대 보존 기간(일)

minRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최소 보존 기간(일)

backupVaultLockCheck(선택 사항), 유형: 문자열

허용되는 값: 'True' 또는 'False'. 리소스가 잠긴 볼트에 백업되어 있는지 확인하는 규칙에 'True'를 입력합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ebs-snapshot-public-restorable-check

Amazon Elastic Block Store(Amazon EBS) 스냅샷을 공개적으로 복원할 수 없는지 확인합니다. RestorableByUserIds 필드가 포함된 하나 이상의 스냅샷이 all로 설정된 경우, 즉 Amazon EBS 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

식별자: EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

트리거 유형: 주기적

AWS 리전: 유럽(스페인) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-capacity-reservation-tagged

Amazon EC2 용량 예약에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_CAPACITY_RESERVATION_TAGGED

리소스 유형: AWS::EC2::CapacityReservation

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-carrier-gateway-tagged

Amazon EC2 통신 사업자 게이트웨이에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_CARRIER_GATEWAY_TAGGED

리소스 유형: AWS::EC2::CarrierGateway

트리거 0유형: 구성 변경

AWS 리전: 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-client-vpn-connection-log-enabled

AWS Client VPN 엔드포인트에 클라이언트 연결 로깅이 활성화되어 있는지 확인합니다. 'Configuration.ConnectionLogOptions.Enabled'가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_CLIENT_VPN_CONNECTION_LOG_ENABLED

리소스 유형: AWS::EC2::ClientVpnEndpoint

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-client-vpn-endpoint-tagged

Amazon EC2 클라이언트 VPN 엔드포인트에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_CLIENT_VPN_ENDPOINT_TAGGED

리소스 유형: AWS::EC2::ClientVpnEndpoint

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-client-vpn-not-authorize-all

AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL

리소스 유형: AWS::EC2::ClientVpnEndpoint

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-dhcp-options-tagged

Amazon EC2 DHCP 옵션에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_DHCP_OPTIONS_TAGGED

리소스 유형: AWS::EC2::DHCPOptions

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-ebs-encryption-by-default

Amazon Elastic Block Store(EBS) 암호화가 기본적으로 활성화되어 있는지 확인합니다. 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_EBS_ENCRYPTION_BY_DEFAULT

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-enis-source-destination-check-enabled

사용자가 관리하는 EC2 ENIs에 소스/대상 검사가 활성화되어 있는지 확인합니다. 'lambda', 'aws_codestar_connections_managed', 'branch', 'efa', 'interface' 및 'quicksight'에 대한 이러한 ENIs에서 소스/대상 검사가 비활성화된 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_ENIS_SOURCE_DESTINATION_CHECK_ENABLED

리소스 유형: AWS::EC2::NetworkInterface

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(서울), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-fleet-tagged

Amazon EC2 플릿에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_FLEET_TAGGED

리소스 유형: AWS::EC2::EC2Fleet

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-imdsv2-check

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터 서비스 버전2(IMDSv2)로 구성되었는지 확인합니다. HttpTokens가 선택 사항으로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_IMDSV2_CHECK

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-instance-detailed-monitoring-enabled

EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_INSTANCE_DETAILED_MONITORING_ENABLED

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-instance-launched-with-allowed-ami

실행 중이거나 중지된 EC2 인스턴스가 허용된 AMIs AMIs)로 시작되었는지 확인합니다. AMI 가 허용된 AMI 기준을 충족하지 않고 허용된 AMIs 설정이 비활성화되지 않은 경우 규칙은 NON_COMPLIANTAMIs.

식별자: EC2_INSTANCE_LAUNCHED_WITH_ALLOWED_AMI

리소스 유형: AWS::EC2::Instance

트리거 유형: 구성 변경 및 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

InstanceStateNameList(선택 사항), 유형: CSV

확인할 규칙에 대한 Amazon EC2 인스턴스 상태의 쉼표로 구분된 목록입니다. 유효한 값은 "실행" 및 "중지"입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-instance-managed-by-systems-manager

> **Important**
>
> 이 규칙의 경우 규칙 식별자(EC2_INSTANCE_MANAGED_BY_SSM)와 규칙 이름(ec2-instance-managed-by-systems-manager)이 서로 다릅니다.

Amazon EC2 인스턴스가 AWS Systems Manager 에이전트(SSM 에이전트)에서 관리되는지 확인합니다. EC2 인스턴스가 실행 중이고 SSM 에이전트가 중지된 경우 또는 EC2 인스턴스가 실행 중이고 SSM 에이전트가 종료된 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> EC2 인스턴스가 중지되고 SSM 에이전트가 실행 중인 경우 규칙은 NON_COMPLIANT를 반환하지 않습니다.

식별자: EC2_INSTANCE_MANAGED_BY_SSM

리소스 유형: AWS::EC2::Instance, AWS::SSM::ManagedInstanceInventory

트리거 0유형: 구성 변경

AWS 리전: 중동(UAE), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-instance-multiple-eni-check

Amazon Elastic Compute Cloud(Amazon EC2)가 여러 탄력적 네트워크 인터페이스(ENI)를 사용하는지 또는 Elastic Fabric Adapter(EFA)를 사용하는지 확인합니다. Amazon EC2 인스턴스가 여러 네트워크 인터페이스를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_INSTANCE_MULTIPLE_ENI_CHECK

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

NetworkInterfaceIds(선택 사항), 유형: CSV

네트워크 인스턴스 ID를 쉼표로 구분한 목록입니다.

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
```

```
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-instance-no-public-ip

EC2 인스턴스에 퍼블릭 IP 연결이 있는지 확인합니다. publicIp 필드가 EC2 인스턴스 구성 항목에 있으면 규칙은 NON_COMPLIANT입니다. 규칙은 IPv4에만 적용됩니다.

컨텍스트: 퍼블릭 IP 주소를 사용하면 인터넷에서 EC2 인스턴스에 직접 액세스할 수 있지만, 보안 또는 규정 준수 관점에서 볼 때 항상 바람직한 것은 아닙니다.

- 보안: 대부분의 경우 퍼블릭 액세스가 필요하지 않는 한 EC2 인스턴스에 퍼블릭 IP 주소를 보유하고 싶지 않을 것입니다. 퍼블릭 IP 주소를 보유하면 EC2 인스턴스가 무단 액세스 또는 공격과 같은 잠재적인 보안 위험에 노출될 수 있습니다.
- 규정 준수: PCI, DSS 또는 HIPAA와 같은 다양한 규정 준수 표준에는 네트워크 세분화 및 액세스 제어와 관련된 특정한 요구 사항이 있습니다. EC2 인스턴스에 불필요한 퍼블릭 IP 주소가 포함되지 않도록 하면 이러한 요구 사항을 준수하는 데 도움이 될 수 있습니다.
- 비용 관리: 퍼블릭 IP 주소는 특히 퍼블릭 IP 주소와 지속적으로 연결된 EC2 인스턴스가 있는 경우 추가 비용을 발생시킬 수 있습니다. 필요하지 않은 퍼블릭 IP가 있는 EC2 인스턴스를 파악하면 잠재적으로 비용을 절감할 수 있습니다.

식별자: EC2_INSTANCE_NO_PUBLIC_IP

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-instance-profile-attached

EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_INSTANCE_PROFILE_ATTACHED

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

IamInstanceProfileArnList(선택 사항), 유형: CSV

> Amazon EC2 인스턴스에 연결할 수 있는 IAM 프로필 Amazon 리소스 이름(ARN)을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-last-backup-recovery-point-created

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 대한 복구 시점이 생성되었는지 확인합니다. 지정된 기간 내에 생성된 해당하는 복구 시점이 Amazon EC2 인스턴스에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_LAST_BACKUP_RECOVERY_POINT_CREATED

리소스 유형: AWS::EC2::Instance

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EC2 인스턴스의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EC2 인스턴스의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 744시간, 일수는 31일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-launch-template-imdsv2-check

Amazon EC2 Launch Template의 현재 설정된 기본 버전이 Amazon EC2 Instance Metadata Service V2(IMDSv2)를 사용하기 위해 새로 시작한 인스턴스를 요구하는지 확인합니다. 'Metadata version'이 V2(IMDSv2)로 지정되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_LAUNCH_TEMPLATE_IMDSV2_CHECK

리소스 유형: AWS::EC2::LaunchTemplate

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이

스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-launch-template-public-ip-disabled

Amazon EC2 시작 템플릿이 네트워크 인터페이스에 퍼블릭 IP 주소를 할당하도록 설정되어 있는지 확인합니다. EC2 시작 템플릿의 기본 버전에 'AssociatePublicIpAddress'가 'true'로 설정된 네트워크 인터페이스가 하나 이상 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

리소스 유형: AWS::EC2::LaunchTemplate

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

exemptedLaunchTemplates(선택 사항), 유형: CSV

AssociatePublicIpAddress 값이 'true'로 설정된 네트워크 인터페이스를 사용할 수 있는 제외된 EC2 시작 템플릿 ID를 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-launch-template-tagged

Amazon EC2 시작 템플릿에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_LAUNCH_TEMPLATE_TAGGED

리소스 유형: AWS::EC2::LaunchTemplate

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-managedinstance-applications-blacklisted

지정 애플리케이션이 인스턴스에 설치되어 있지 않은지 확인합니다. 필요한 경우 버전을 지정할 수도 있습니다. 최신 버전은 거부 목록에 포함되지 않습니다. 필요한 경우 플랫폼을 지정하여 해당 플랫폼을 실행 중인 인스턴스에만 규칙을 적용할 수 있습니다.

식별자: EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

리소스 유형: AWS::SSM::ManagedInstanceInventory

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

applicationNames, 유형: CSV

애플리케이션 이름을 쉼표로 구분한 목록입니다. 선택에 따라 ':'을 붙여 버전을 지정할 수 있습니다 (예: 'Chrome:0.5.3, Firefox').

> **Note**
>
> 애플리케이션 이름이 정확하게 일치해야 합니다. 예를 들어 Linux에서는 **`firefox`**를 사용하고, Amazon Linux에서는 **`firefox-compat`**를 사용합니다. 또한 AWS Config 는 현재 applicationNames 파라미터(예: **`firefox*`**)에 대한 와일드카드를 지원하지 않습니다.

platformType(선택 사항), 유형: 문자열

플랫폼 유형(예: 'Linux' 또는 'Windows')입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-managedinstance-applications-required

지정 애플리케이션이 인스턴스에 모두 설치되어 있는지 확인합니다. 선택적으로, 허용되는 최소 버전을 지정할 수 있습니다. 플랫폼을 지정하여 해당 플랫폼을 실행 중인 인스턴스에만 규칙을 적용할 수도 있습니다.

> **Note**
>
> SSM Agent가 EC2 인스턴스에서 실행 중이고, 애플리케이션 소프트웨어 인벤토리를 수집하기 위한 연결이 생성되었는지 확인합니다. SSM 에이전트가 설치되지 않았거나 연결이 아직 생성되거나 실행되지 않은 `NOT_APPLICABLE` 경우 규칙이를 반환합니다.

식별자: EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED

리소스 유형: AWS::SSM::ManagedInstanceInventory

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

applicationNames, 유형: CSV

애플리케이션 이름을 쉼표로 구분한 목록입니다. 선택에 따라 ':'을 붙여 버전을 지정할 수 있습니다(예: 'Chrome:0.5.3, Firefox').

> **Note**
>
> 애플리케이션 이름이 정확하게 일치해야 합니다. 예를 들어 Linux에서는 **`firefox`**를 사용하고, Amazon Linux에서는 **`firefox-compat`**를 사용합니다. 또한 AWS Config 는 현재 applicationNames 파라미터(예:)에 대한 와일드카드를 지원하지 않습니다**`firefox*`**.

platformType(선택 사항), 유형: 문자열

플랫폼 유형(예: 'Linux' 또는 'Windows')입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-managedinstance-association-compliance-status-check

인스턴스에서 연결을 실행한 후 AWS Systems Manager 연결 규정 준수 상태가 COMPLIANT 또는 NON_COMPLIANT인지 확인합니다. 필드 상태가 COMPLIANT이면 규칙이 규정 준수로 간주됩니다. 연결에 대한 자세한 내용은 연결이란 무엇인가요?를 참조하세요.

식별자: EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

리소스 유형: AWS::SSM::AssociationCompliance

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-managedinstance-inventory-blacklisted

Amazon EC2 Systems Manager가 관리하는 인스턴스가 블랙리스트상의 인벤토리 유형을 수집하도록 구성되어 있는지 확인합니다.

식별자: EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED

리소스 유형: AWS::SSM::ManagedInstanceInventory

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

inventoryNames, 유형: CSV

Systems Manager 인벤토리 유형의 쉼표로 구분된 목록(예: 'AWS:Network, AWS:WindowsUpdate').

platformType(선택 사항), 유형: 문자열

플랫폼 유형(예: 'Linux')입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-managedinstance-patch-compliance-status-check

인스턴스에 패치를 설치한 후 AWS Systems Manager 패치 규정 준수의 규정 준수 상태가 COMPLIANT 또는 NON_COMPLIANT인지 확인합니다. 필드 상태가 COMPLIANT이면 규칙이 규정 준수로 간주됩니다.

식별자: EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

리소스 유형: AWS::SSM::PatchCompliance

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(오사카), 유럽(밀라노), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-managedinstance-platform-check

EC2 관리형 인스턴스의 구성이 바람직한지 확인합니다.

식별자: EC2_MANAGEDINSTANCE_PLATFORM_CHECK

리소스 유형: AWS::SSM::ManagedInstanceInventory

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

platformType, 유형: 문자열

플랫폼 유형(예: 'Linux')입니다.

platformVersion(선택 사항), 유형: 문자열

플랫폼 버전(예: '2016.09')입니다.

agentVersion(선택 사항), 유형: 문자열

에이전트 버전(예: '2.0.433.0')입니다.

platformName(선택 사항), 유형: 문자열

플랫폼의 버전(예: '2016.09')입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-meets-restore-time-target

Amazon Elastic Compute Cloud(Amazon EC2)의 복원 시간이 지정된 기간을 충족하는지 확인합니다. Amazon EC2 인스턴스의 LatestRestoreExecutionTimeMinutes가 maxRestoreTime(분)보다 큰 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_MEETS_RESTORE_TIME_TARGET

리소스 유형: AWS::EC2::Instance

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

maxRestoreTime, 유형: int

허용되는 최대 복원 런타임의 숫자 값입니다.

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EC2 인스턴스의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EC2 인스턴스의 ID입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-network-insights-access-scope-analysis-tagged

Amazon EC2 네트워크 인사이트 액세스 범위 분석에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_NETWORK_INSIGHTS_ACCESS_SCOPE_ANALYSIS_TAGGED

리소스 유형: AWS::EC2::NetworkInsightsAccessScopeAnalysis

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-network-insights-access-scope-tagged

Amazon EC2 네트워크 인사이트 액세스 범위에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_NETWORK_INSIGHTS_ACCESS_SCOPE_TAGGED

리소스 유형: AWS::EC2::NetworkInsightsAccessScope

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-network-insights-path-tagged

Amazon EC2 네트워크 인사이트 경로에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_NETWORK_INSIGHTS_PATH_TAGGED

리소스 유형: AWS::EC2::NetworkInsightsPath

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-no-amazon-key-pair

Amazon Elastic Compute Cloud(EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되었는지 확인합니다. 실행 중인 EC2 인스턴스가 키 페어를 사용하여 시작된 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_NO_AMAZON_KEY_PAIR

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-paravirtual-instance-check

EC2 인스턴스의 가상화 유형이 반가상인지 확인합니다. 'virtualizationType'이 'paravirtual'으로 설정된 경우 이 규칙은 EC2 인스턴스에 대해 NON_COMPLIANT입니다.

식별자: EC2_PARAVIRTUAL_INSTANCE_CHECK

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능합니다.

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-prefix-list-tagged

Amazon EC2 관리형 접두사 목록에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_PREFIX_LIST_TAGGED

리소스 유형: AWS::EC2::PrefixList

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-resources-in-logically-air-gapped-vault

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스가 논리적 에어 갭 저장소에 있는지 확인합니다. Amazon EC2 인스턴스가 지정된 기간 내에 논리적 에어 갭 저장소에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

리소스 유형: AWS::EC2::Instance

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EC2 인스턴스의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EC2 인스턴스의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 2184시간, 일수는 91일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-resources-protected-by-backup-plan

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스가 백업 계획에 의해 보호되는지 확인합니다. Amazon EC2 인스턴스를 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
> 이 규칙은 실행 중인 Amazon EC2 인스턴스에만 적용되며 전원이 꺼진 인스턴스에는 적용되지 않습니다.

식별자: EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN

리소스 유형: AWS::EC2::Instance

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EC2 인스턴스의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EC2 인스턴스의 ID입니다.

crossRegionList(선택 사항), 유형: 문자열

리전 간 백업 사본을 보관할 대상 리전을 쉼표로 구분한 목록입니다.

crossAccountList(선택 사항), 유형: 문자열

계정 간 백업 사본을 보관할 대상 계정을 쉼표로 구분한 목록입니다.

maxRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최대 보존 기간(일)

minRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최소 보존 기간(일)

backupVaultLockCheck(선택 사항), 유형: 문자열

허용되는 값: 'True' 또는 'False'. 리소스가 잠긴 볼트에 백업되어 있는지 확인하는 규칙에 'True'를 입력합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-security-group-attached-to-eni

기본이 아닌 보안 그룹이 탄력적 네트워크 인터페이스에 연결되어 있는지 확인합니다. 보안 그룹이 네트워크 인터페이스와 연결되어 있지 않으면 규칙은 NON_COMPLIANT입니다.

식별자: EC2_SECURITY_GROUP_ATTACHED_TO_ENI

리소스 유형: AWS::EC2::SecurityGroup

트리거 0유형: 구성 변경

AWS 리전: 중동(UAE), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-security-group-attached-to-eni-periodic

기본이 아닌 보안 그룹이 탄력적 네트워크 인터페이스(ENI)에 연결되어 있는지 확인합니다. 보안 그룹이 ENI와 연결되어 있지 않으면 규칙은 NON_COMPLIANT입니다. 호출 계정이 소유하지 않은 보안 그룹은 NOT_APPLICABLE로 평가됩니다.

> **Note**
>
> 이 규칙은 `AWS::EC2::SecurityGroup` 리소스 유형에 대해 보고합니다. 하지만 규칙을 효과적으로 실행하려면 `AWS::EC2::NetworkInterface` 리소스 유형의 기록을 활성화해야 합니다.

식별자: EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC

리소스 유형: AWS::EC2::SecurityGroup

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-spot-fleet-request-ct-encryption-at-rest

Amazon EC2 스팟 플릿 요청에 시작된 모든 EC2 인스턴스에 대해 암호화된 Amazon Elastic Block Store(Amazon EBS) 볼륨이 있는지 확인합니다. EBS 볼륨이 저장 시 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_SPOT_FLEET_REQUEST_CT_ENCRYPTION_AT_REST

리소스 유형: AWS::EC2::SpotFleet

트리거 0유형: 구성 변경

AWS 리전: 유럽(아일랜드), 미국 동부(버지니아 북부), 아시아 태평양(서울), 미국 서부(오레곤), 중국(닝샤), 유럽(취리히) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-stopped-instance

허용된 일수를 초과하여 중지된 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스가 있는지 확인합니다. Amazon EC2 인스턴스가 허용된 일수보다 오래 중지된 상태인 경우 또는 시간을 확인할 수 없는 경우 규칙은 NON_COMPLIANT입니다.

Identifier: EC2_STOPPED_INSTANCE

리소스 유형: AWS::EC2::Instance

트리거 유형: 주기적

AWS 리전: 아프리카(케이프타운), 중동(UAE), 아시아 태평양(오사카), 아시아 태평양(멜버른), 유럽(밀라노), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

AllowedDays(선택 사항), 유형: int, 기본값: 30

규칙이 NON_COMPLIANT가 되기까지 Amazon EC2 인스턴스가 중지된 상태로 유지될 수 있는 일수입니다. 기본 일수는 30일입니다.

> **Note**
>
> 이 규칙은 수집된 기록 데이터에 기반하므로 선택한 일수는 구성된 보존 기간보다 짧아야 합니다. 기록 데이터 보존에 대한 자세한 내용은 AWS Config 데이터 삭제를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-token-hop-limit-check

Amazon Elastic Compute Cloud(EC2) 인스턴스 메타데이터에 원하는 제한보다 낮은 토큰 홉 제한이 지정되어 있는지 확인합니다. 인스턴스의 홉 제한 값이 원하는 제한을 초과할 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_TOKEN_HOP_LIMIT_CHECK

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

tokenHopLimit(선택 사항), 유형: int

원하는 토큰 홉 제한입니다. 유효한 값은 1~64 사이입니다. 파라미터가 지정되지 않을 경우 기본값은 1입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-traffic-mirror-filter-description

Amazon EC2 트래픽 미러 필터에 설명이 있는지 확인합니다. configuration.Description이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_TRAFFIC_MIRROR_FILTER_DESCRIPTION

리소스 유형: AWS::EC2::TrafficMirrorFilter

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-traffic-mirror-filter-tagged

Amazon EC2 트래픽 미러 필터에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_TRAFFIC_MIRROR_FILTER_TAGGED

리소스 유형: AWS::EC2::TrafficMirrorFilter

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-traffic-mirror-session-description

Amazon EC2 트래픽 미러 세션에 설명이 있는지 확인합니다. configuration.Description이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_TRAFFIC_MIRROR_SESSION_DESCRIPTION

리소스 유형: AWS::EC2::TrafficMirrorSession

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 유럽(밀라노), AWS GovCloud(미국

동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-traffic-mirror-session-tagged

Amazon EC2 트래픽 미러 세션에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_TRAFFIC_MIRROR_SESSION_TAGGED

리소스 유형: AWS::EC2::TrafficMirrorSession

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-traffic-mirror-target-description

Amazon EC2 트래픽 미러 대상에 설명이 있는지 확인합니다. configuration.Description이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_TRAFFIC_MIRROR_TARGET_DESCRIPTION

리소스 유형: AWS::EC2::TrafficMirrorTarget

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-traffic-mirror-target-tagged

Amazon EC2 트래픽 미러 대상에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_TRAFFIC_MIRROR_TARGET_TAGGED

리소스 유형: AWS::EC2::TrafficMirrorTarget

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-transit-gateway-auto-vpc-attach-disabled

Amazon Elastic Compute Cloud(Amazon EC2) Tranit Gateways에 'AutoAcceptSharedAttachments'가 활성화되어 있는지 확인합니다. 'AutoAcceptSharedAttachments'가 '활성화'로 설정된 경우 Transit Gateway의 규칙은 NON_COMPLIANT입니다.

식별자: EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED

리소스 유형: AWS::EC2::TransitGateway

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-transit-gateway-multicast-domain-tagged

Amazon EC2 전송 게이트웨이 멀티캐스트 도메인에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EC2_TRANSIT_GATEWAY_MULTICAST_DOMAIN_TAGGED

리소스 유형: AWS::EC2::TransitGatewayMulticastDomain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-volume-inuse-check

EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 선택적으로, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.

실행 중인 EC2 인스턴스에 EBS 볼륨이 연결된 경우 규칙은 COMPLIANT입니다. 이때 EC2 인스턴스에서 EBS 볼륨을 능동적으로 사용하고 있는 경우에는 규칙이 COMPLIANT입니다.

EBS 볼륨이 어떤 EC2 인스턴스에도 연결되지 않았거나, 중지 또는 종료된 EC2 인스턴스에 연결된 경우 규칙은 NON_COMPLIANT입니다. 이때 EC2 인스턴스에서 EBS 볼륨을 능동적으로 사용하고 있지 않을 경우에는 규칙이 NON_COMPLIANT입니다.

식별자: EC2_VOLUME_INUSE_CHECK

리소스 유형: AWS::EC2::Volume

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

deleteOnTermination(선택 사항), 유형: boolean

인스턴스 종료 시, EBS 볼륨이 삭제 대기 상태가 됩니다. 가능한 값: True 또는 False(다른 입력 값은 NON_COMPLIANT로 표시됨). `True`로 설정하면 종료된 EBS 볼륨이 삭제 대상으로 표시되지 않은 경우 규칙은 NON_COMPLIANT가 됩니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-vpn-connection-logging-enabled

AWS Site-to-Site VPN 연결에 두 터널 모두에 대해 Amazon CloudWatch 로깅이 활성화되어 있는지 확인합니다. Site-to-Site VPN 연결에서 두 터널 중 하나라도 Amazon CloudWatch 로깅이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: EC2_VPN_CONNECTION_LOGGING_ENABLED

리소스 유형: AWS::EC2::VPNConnection

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecr-private-image-scanning-enabled

Amazon Elastic Container Registry(Amazon ECR) 리포지토리에 이미지 스캔이 활성화되어 있는지 확인합니다. 프라이빗 Amazon ECR 리포지토리의 스캔 빈도가 푸시할 때 스캔 또는 연속 스캔에 대한 것이 아닐 경우 규칙은 NON_COMPLIANT입니다. 이미지 스캔에 대한 자세한 내용은 Amazon ECR 사용 설명서의 이미지 스캔을 참조하세요.

식별자: ECR_PRIVATE_IMAGE_SCANNING_ENABLED

리소스 유형: AWS::ECR::Repository

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecr-private-lifecycle-policy-configured

프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

리소스 유형: AWS::ECR::Repository

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecr-private-tag-immutability-enabled

Amazon Elastic Container Registry(ECR) 리포지토리에 태그 변경 불가능이 활성화되어 있는지 확인합니다. 프라이빗 ECR 리포지토리에 대해 태그 변경 불가능이 활성화되지 않은 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

리소스 유형: AWS::ECR::Repository

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecr-repository-cmk-encryption-enabled

고객 관리형 KMS 키를 사용하여 ECR 리포지토리가 저장 시 암호화되었는지 확인합니다. 리포지토리가 AES256 또는 기본 KMS 키('aws/ecr')를 사용하여 암호화된 경우이 규칙은 NON_COMPLIANT입니다.

식별자: ECR_REPOSITORY_CMK_ENCRYPTION_ENABLED

리소스 유형: AWS::ECR::Repository

트리거 0유형: 구성 변경

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: CSV

ECR 리포지토리를 암호화하기 위한 KMS 키 Amazon 리소스 이름(ARNs)의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecr-repository-tagged

Amazon ECR 리포지토리에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: ECR_REPOSITORY_TAGGED

리소스 유형: AWS::ECR::Repository

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-awsvpc-networking-enabled

활성 ECSTaskDefinitions의 네트워킹 모드가 'awsvpc'로 설정되어 있는지 확인합니다. 활성 ECSTaskDefinitions 'awsvpc'로 설정되지 않은 경우 이 규칙은 NON_COMPLIANT입니다.

> **Note**
> 이 규칙은 Amazon ECS 태스크 정의의 최신 활성 버전만 평가합니다.

식별자: ECS_AWSVPC_NETWORKING_ENABLED

리소스 유형: AWS::ECS::TaskDefinition

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-containers-nonprivileged

ECSTaskDefinitions의 컨테이너 정의에 있는 권한 있는 파라미터가 'true'로 설정되어 있는지 확인합니다. 권한이 있는 파라미터가 'true'인 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
> 이 규칙은 Amazon ECS 태스크 정의의 최신 활성 버전만 평가합니다.

식별자: ECS_CONTAINERS_NONPRIVILEGED

리소스 유형: AWS::ECS::TaskDefinition

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-containers-readonly-access

Amazon Elastic Container Service(Amazon ECS)의 컨테이너에 루트 파일 시스템에 대한 읽기 전용 액세스 권한만 있는지 확인합니다. ECSTaskDefinitions의 컨테이너 정의에 있는 readonlyRootFilesystem 파라미터가 'false'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 이 규칙은 Amazon ECS 태스크 정의의 최신 활성 버전만 평가합니다.

식별자: ECS_CONTAINERS_READONLY_ACCESS

리소스 유형: AWS::ECS::TaskDefinition

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-container-insights-enabled

Amazon Elastic Container Service 클러스터에 컨테이너 인사이트가 활성화되어 있는지 확인합니다. 컨테이너 인사이트가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: ECS_CONTAINER_INSIGHTS_ENABLED

리소스 유형: AWS::ECS::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-fargate-latest-platform-version

ECS Fargate 서비스가 최신 플랫폼 버전으로 설정되어 있는지 확인합니다. Fargate 시작 유형의 PlatformVersion이 LATEST로 설정되어 있지 않거나, LatestLinuxVersion 또는 `latestWindowsVersion`이 파라미터로 제공되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: ECS_FARGATE_LATEST_PLATFORM_VERSION

리소스 유형: AWS::ECS::Service

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

latestLinuxVersion(선택 사항), 유형: 문자열

최신 Linux는 의미 체계 버전 관리(SemVer) 형식의 'PlatformVersion'을 지원했습니다. Fargate가 배포되고 'PlatformVersion'이 명시적으로 지정되었거나 CodeDeploy가 'DeploymentController'로 사용되는 경우 파라미터가 필요할 수 있습니다.

latestWindowsVersion(선택 사항), 유형: 문자열

최신 Windows는 의미 체계 버전 관리(SemVer) 형식의 'PlatformVersion'을 지원했습니다. Fargate가 배포되고 'PlatformVersion'이 명시적으로 지정되었거나 CodeDeploy가 'DeploymentController'로 사용되는 경우 파라미터가 필요할 수 있습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-no-environment-secrets

보안 암호가 컨테이너 환경 변수로 전달되는지 확인합니다. 하나 이상의 환경 변수 키가 `'secretKeys'` 파라미터에 나열된 키와 일치하는 경우 규칙은 NON_COMPLIANT입니다(Amazon S3와 같은 다른 위치의 환경 변수는 제외).

> **Note**
> 이 규칙은 Amazon ECS 태스크 정의의 최신 활성 버전만 평가합니다.

식별자: ECS_NO_ENVIRONMENT_SECRETS

리소스 유형: AWS::ECS::TaskDefinition

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

secretKeys, 유형: CSV

태스크 정의 내에 있는 컨테이너 정의의 환경 변수에서 검색할 키 이름을 쉼표로 구분한 목록입니다. 추가 공백은 제거됩니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-task-definition-log-configuration

활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

> **Note**
> 이 규칙은 Amazon ECS 태스크 정의의 최신 활성 버전만 평가합니다.

식별자: ECS_TASK_DEFINITION_LOG_CONFIGURATION

리소스 유형: AWS::ECS::TaskDefinition

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-task-definition-memory-hard-limit

Amazon Elastic Container Service(ECS) 태스크 정의에 컨테이너 정의를 위해 설정된 메모리 제한이 있는지 확인합니다. 한 컨테이너 정의에 대해 'memory' 파라미터가 없는 경우 태스크 정의의 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 이 규칙은 Amazon ECS 태스크 정의의 최신 활성 버전만 평가합니다.

식별자: ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

리소스 유형: AWS::ECS::TaskDefinition

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-task-definition-network-mode-not-host

Amazon ECS 태스크 정의의 최신 활성 개정이 호스트 네트워크 모드를 사용하는지 확인합니다. ECS 태스크 정의의 최신 활성 개정에서 호스트 네트워크 모드를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

식별자: ECS_TASK_DEFINITION_NETWORK_MODE_NOT_HOST

리소스 유형: AWS::ECS::TaskDefinition

트리거 0유형: 구성 변경

AWS 리전: 중동(바레인), 아시아 태평양(태국), 멕시코(중부) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-task-definition-nonroot-user

ECSTaskDefinitions가 Amazon Elastic Container Service(Amazon ECS) EC2 시작 유형 컨테이터를 실행할 사용자를 지정하는지 확인합니다. 'user' 파라미터가 없거나 'root'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
> 이 규칙은 Amazon ECS 태스크 정의의 최신 활성 버전만 평가합니다.

식별자: ECS_TASK_DEFINITION_NONROOT_USER

리소스 유형: AWS::ECS::TaskDefinition

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-task-definition-pid-mode-check

ECSTaskDefinitions가 호스트의 프로세스 네임스페이스를 Amazon Elastic Container Service(Amazon ECS) 컨테이너와 공유하도록 구성되어 있는지 확인합니다. pidMode 파라미터가 'host'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
> 이 규칙은 Amazon ECS 태스크 정의의 최신 활성 버전만 평가합니다.

식별자: ECS_TASK_DEFINITION_PID_MODE_CHECK

리소스 유형: AWS::ECS::TaskDefinition

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ecs-task-definition-user-for-host-mode-check

호스트 네트워크 모드가 있는 Amazon ECS 태스크 정의에 컨테이너 정의에 권한이 있거나 루트가 아닌지 확인합니다. 태스크 정의의 최신 활성 개정에 privileged=false(또는 null) 및 user=root(또는 null)가 있는 경우 규칙은 NON_COMPLIANT입니다.

> **Important**
> 규칙을 준수 상태로 반환하려면 하나의 조건만 충족하면 됩니다.
> 다음 시나리오에서 규칙은 COMPLIANT입니다.
>
> - 네트워크 모드가 호스트로 설정되지 않은 경우,

- 태스크 정의의 최신 활성 개정에 privileged=true가 있는 경우,
- 태스크 정의의 최신 활성 개정에 루트가 아닌 사용자가 있는 경우.

즉, 규칙을 준수 상태로 반환하려면 이러한 조건 중 하나만 충족하면 됩니다. 태스크 정의에 privileged=true가 있는지 구체적으로 확인하려면 ecs-containers-nonprivileged를 참조하세요. 태스크 정의에 루트가 아닌 사용자가 있는지 구체적으로 확인하려면 ecs-task-definition-nonroot-user를 참조하세요.

식별자: ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

리소스 유형: AWS::ECS::TaskDefinition

트리거 0유형: 구성 변경

AWS 리전: 중동(UAE), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

SkipInactiveTaskDefinitions(선택 사항), 유형: boolean

비활성 Amazon EC2 태스크 정의를 확인하지 않도록 하는 부울 플래그입니다. 'true'로 설정하면 규칙이 비활성 Amazon EC2 태스크 정의를 평가하지 않습니다. 'false'로 설정하면 규칙이 비활성 Amazon EC2 태스크 정의의 최신 버전을 평가합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

efs-access-point-force-root-directory

Amazon Elastic File System(Amazon EFS)의 액세스 포인트가 루트 디렉터리를 적용하도록 구성되어 있는지 확인합니다. 'Path' 값이 '/'(파일 시스템의 기본 루트 디렉터리)로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

리소스 유형: AWS::EFS::AccessPoint

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

approvedDirectories(선택 사항), 유형: CSV

Amazon EFS 액세스 포인트 루트 디렉터리 적용을 위해 승인된 하위 디렉터리 경로를 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

efs-access-point-enforce-user-identity

Amazon Elastic File System(Amazon EFS)의 액세스 포인트가 사용자 자격 증명을 적용하도록 구성되어 있는지 확인합니다. 'PosixUser'가 정의되지 않은 경우 또는 파라미터가 제공되었으나 해당 파라미터에 일치하는 항목이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY

리소스 유형: AWS::EFS::AccessPoint

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

approvedUids(선택 사항), 유형: CSV

EFS 액세스 포인트 사용자 적용을 위해 승인된 POSIX 사용자 ID를 쉼표로 구분한 목록입니다.

approvedGids(선택 사항), 유형: CSV

EFS 액세스 포인트 사용자 적용을 위해 승인된 POSIX 그룹 ID를 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

efs-automatic-backups-enabled

Amazon Elastic File System(Amazon EFS) 파일 시스템에 자동 백업이 활성화되어 있는지 확인합니다. `BackupPolicy.Status`가 DISABLED로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: EFS_AUTOMATIC_BACKUPS_ENABLED

리소스 유형: AWS::EFS::FileSystem

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

efs-encrypted-check

Amazon Elastic File System(Amazon EFS)이 AWS Key Management Service ()를 사용하여 파일 데이터를 암호화하도록 구성되어 있는지 확인합니다AWS KMS. 암호화된 키가 `DescribeFileSystems`에서 false로 설정되거나 `DescribeFileSystems`의 `KmsKeyId` 키가 `KmsKeyId` 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다.

식별자: EFS_ENCRYPTED_CHECK

리소스 유형: AWS::EFS::FileSystem

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

KmsKeyId(선택 사항), 유형: 문자열

EFS 파일 시스템을 암호화하는 데 사용되는 KMS 키의 Amazon 리소스 이름(ARN)입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

efs-filesystem-ct-encrypted

Amazon Elastic File System(Amazon EFS)이 AWS Key Management Service(AWS KMS)를 사용하여 데이터를 암호화하는지 확인합니다. 파일 시스템이 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다. 필요한 경우, 파일 시스템이 지정된 KMS 키로 암호화되지 않았는지 확인할 수 있습니다.

식별자: EFS_FILESYSTEM_CT_ENCRYPTED

리소스 유형: AWS::EFS::FileSystem

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: 문자열

(선택 사항) AWS KMS 키에 대한 Amazon 리소스 이름(ARNs)의 쉼표로 구분된 목록입니다. 제공된 경우, 규칙이 지정된 KMS 키가 Amazon EFS 파일 시스템을 암호화하지 않는지 확인합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

efs-in-backup-plan

AWS 백업의 백업 계획에 Amazon Elastic File System(Amazon EFS) 파일 시스템이 추가되었는지 확인합니다. EFS 파일 시스템이 백업 계획에 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: EFS_IN_BACKUP_PLAN

리소스 유형: AWS::EFS::FileSystem

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

efs-last-backup-recovery-point-created

Amazon Elastic File System(Amazon EFS)의 복구 시점이 생성되었는지 확인합니다. 지정된 기간 내에 생성된 해당하는 복구 시점이 Amazon EFS 파일 시스템에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

리소스 유형: AWS::EFS::FileSystem

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EFS 파일 시스템의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 EFS 파일 시스템의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 744시간, 일수는 31일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

efs-meets-restore-time-target

Amazon Elastic File System(Amazon EFS) 파일 시스템의 복원 시간이 지정된 기간을 충족하는지 확인합니다. Amazon EFS 파일 시스템의 LatestRestoreExecutionTimeMinutes가 maxRestoreTime(분)보다 큰 경우 규칙은 NON_COMPLIANT입니다.

식별자: EFS_MEETS_RESTORE_TIME_TARGET

리소스 유형: AWS::EFS::FileSystem

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

maxRestoreTime, 유형: int

허용되는 최대 복원 런타임의 숫자 값입니다.

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EFS 파일 시스템의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 EFS 파일 시스템의 ID입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

efs-mount-target-public-accessible

Amazon Elastic File System(Amazon EFS) 탑재 대상이 퍼블릭 서브넷과 연결되어 있지 않은지 확인합니다. Amazon EFS 탑재 대상이 퍼블릭 서브넷과 연결된 경우 규칙은 NON-COMPLIANT입니다.

식별자: EFS_MOUNT_TARGET_PUBLIC_ACCESSIBLE

리소스 유형: AWS::EFS::FileSystem

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

efs-resources-in-logically-air-gapped-vault

Amazon Elastic File System(Amazon EFS) 파일 시스템이 논리적 에어 갭 저장소에 있는지 확인합니다. Amazon Elastic File System(Amazon EFS) 파일 시스템이 지정된 기간 내에 논리적 에어 갭 저장소에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EFS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

리소스 유형: AWS::EFS::FileSystem

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon EFS 파일 시스템의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 EFS 파일 시스템의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 2184시간, 일수는 91일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

efs-resources-protected-by-backup-plan

Amazon Elastic File System(Amazon EFS) 파일 시스템이 백업 계획에 의해 보호되는지 확인합니다. EFS 파일 시스템을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

리소스 유형: AWS::EFS::FileSystem

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 EFS 파일 시스템의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 EFS 파일 시스템의 ID입니다.

crossRegionList(선택 사항), 유형: 문자열

리전 간 백업 사본을 보관할 대상 리전을 쉼표로 구분한 목록입니다.

crossAccountList(선택 사항), 유형: 문자열

계정 간 백업 사본을 보관할 대상 계정을 쉼표로 구분한 목록입니다.

maxRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최대 보존 기간(일)

minRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최소 보존 기간(일)

backupVaultLockCheck(선택 사항), 유형: 문자열

허용되는 값: 'True' 또는 'False'. 리소스가 잠긴 볼트에 백업되어 있는지 확인하는 규칙에 'True'를 입력합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

eip-attached

AWS 계정에 할당된 모든 탄력적 IP 주소가 EC2 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되어 있는지 확인합니다. 탄력적 IP 주소의 'AssociationId'가 null인 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
> 평과 결과가 나올 때까지 최대 6시간이 걸릴 수 있습니다.

식별자: EIP_ATTACHED

리소스 유형: AWS::EC2::EIP

트리거 0유형: 구성 변경

AWS 리전: 중동(UAE) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
}
...
```

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

eks-cluster-logging-enabled

Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: EKS_CLUSTER_LOGGING_ENABLED

리소스 유형: AWS::EKS::Cluster

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

eks-cluster-log-enabled

Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 활성화되지 않았거나, 언급된 로그 유형으로 로깅이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: EKS_CLUSTER_LOG_ENABLED

리소스 유형: AWS::EKS::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

logTypes(선택 사항), 유형: CSV

> 확인할 규칙에 대한 EKS 클러스터 컨트롤 플레인 로그 유형의 쉼표로 구분된 목록입니다. 유효한 값: "api", "audit", "authenticator", "controllerManager", "scheduler

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

eks-cluster-oldest-supported-version

Amazon Elastic Kubernetes Service(EKS) 클러스터가 지원되는 가장 오래된 버전을 실행하고 있는지 확인합니다. EKS 클러스터가 지원되는 가장 오래된 버전(파라미터 '`oldestVersionSupported`'와 같음)을 실행하는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EKS_CLUSTER_OLDEST_SUPPORTED_VERSION

리소스 유형: AWS::EKS::Cluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

oldestVersionSupported, 유형: 문자열

AWS에서 지원되는 가장 오래된 Kubernetes 버전의 값입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

eks-cluster-secrets-encrypted

Amazon EKS 클러스터가 KMS를 사용하여 암호화된 AWS Kubernetes 보안 암호를 갖도록 구성되어 있는지 확인합니다. EKS 클러스터에 encryptionConfig 리소스가 없거나 encryptionConfig이 리소스를 보안 키로 명명하지 않은 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: EKS_CLUSTER_SECRETS_ENCRYPTED

리소스 유형: AWS::EKS::Cluster

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: CSV

EKS 사용에 대해 승인된 KMS 키 Amazon 리소스 이름(ARN)의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

eks-cluster-supported-version

Amazon Elastic Kubernetes Service(EKS) 클러스터가 지원되는 가장 오래된 Kubernetes 버전을 실행하고 있는지 확인합니다. EKS 클러스터가 지원되지 않는 버전(파라미터 '`oldestVersionSupported`' 미만)을 실행하고 있는 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: EKS_CLUSTER_SUPPORTED_VERSION

리소스 유형: AWS::EKS::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

oldestVersionSupported, 유형: 문자열

AWS에서 지원되는 가장 오래된 Kubernetes 버전의 값입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

eks-endpoint-no-public-access

Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트가 퍼블릭 액세스 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.

식별자: EKS_ENDPOINT_NO_PUBLIC_ACCESS

리소스 유형: AWS::EKS::Cluster

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

eks-secrets-encrypted

Amazon Elastic Kubernetes Service 클러스터가 AWS Key Management Service (KMS) 키를 사용하여 암호화된 Kubernetes 보안 암호를 갖도록 구성되어 있는지 확인합니다.

- EKS 클러스터에 보안 암호가 리소스 중 하나로 포함된 encryptionConfig가 있는 경우 이 규칙은 COMPLIANT입니다.
- EKS 보안 암호를 암호화하는 데 사용된 키가 파라미터와 일치하는 경우에도 이 규칙은 COMPLIANT입니다.
- EKS 클러스터에 encryptionConfig가 없거나 encryptionConfig 리소스에 보안 암호가 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
- EKS 보안 암호를 암호화하는 데 사용된 키가 파라미터와 일치하는 경우에도 이 규칙은 COMPLIANT입니다.

식별자: EKS_SECRETS_ENCRYPTED

리소스 유형: AWS::EKS::Cluster

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: CSV

EKS 클러스터의 암호화된 보안 암호에 사용해야 하는 KMS 키의 쉼표로 구분된 Amazon 리소스 이름(ARN) 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticache-auto-minor-version-upgrade-check

Amazon ElastiCache 클러스터에 마이너 버전 자동 업그레이드가 활성화되어 있는지 확인합니다. Redis 또는 Valkey 엔진을 사용하고 'AutoMinorVersionUpgrade'가 'true'로 설정되지 않은 경우 ElastiCache 클러스터의 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

리소스 유형: AWS::ElastiCache::CacheCluster

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticache-rbac-auth-enabled

Amazon ElastiCache 복제 그룹에 RBAC 인증이 활성화되어 있는지 확인합니다. Redis 버전이 6 이상이고 'UserGroupIds'가 없거나, 비어 있거나, '`allowedUserGroupIDs`' 파라미터에서 제공된 항목과 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICACHE_RBAC_AUTH_ENABLED

리소스 유형: AWS::ElastiCache::ReplicationGroup

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

allowedUserGroupIDs(선택 사항), 유형: CSV

ElastiCache 복제 그룹 액세스가 승인된 사용자 그룹 ID를 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticache-redis-cluster-automatic-backup-check

Amazon ElastiCache Redis 클러스터에 자동 백업이 설정되어 있는지 확인합니다. Redis 클러스터에 대한 SnapshotRetentionLimit가 SnapshotRetentionPeriod 파라미터보다 작으면 규칙은 NON_COMPLIANT입니다. 예를 들어 파라미터가 15인 경우 snapshotRetentionPeriod가 0~15이면 규칙이 NON_COMPLIANT입니다.

식별자: ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

리소스 유형: AWS::ElastiCache::CacheCluster, AWS::ElastiCache::ReplicationGroup

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

snapshotRetentionPeriod(선택 사항), 유형: int, 기본값: 15

Redis 클러스터의 최소 스냅샷 보존 기간(일)입니다. 기본값은 15일입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticache-repl-grp-auto-failover-enabled

Amazon ElastiCache Redis 복제 그룹에 자동 장애 조치가 활성화되어 있는지 확인합니다. 'AutomaticFailover'가 'enabled'로 설정되어 있지 않은 경우 ElastiCache 복제 그룹에 대한 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

리소스 유형: AWS::ElastiCache::ReplicationGroup

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticache-repl-grp-encrypted-at-rest

Amazon ElastiCache 복제 그룹에 저장 시 암호화가 활성화되어 있는지 확인합니다. 'AtRestEncryptionEnabled'가 비활성화되어 있거나, KMS 키 ARN이 approvedKMSKeyArns 파라미터와 일치하지 않는 경우 ElastiCache 복제 그룹에 대한 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

리소스 유형: AWS::ElastiCache::ReplicationGroup

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

approvedKMSKeyIds(선택 사항), 유형: CSV

ElastiCache 사용이 승인된 KMS 키 ID를 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticache-repl-grp-encrypted-in-transit

Amazon ElastiCache 복제 그룹에 전송 시 암호화가 활성화되어 있는지 확인합니다. 'TransitEncryptionEnabled'가 'false'로 설정되어 있는 경우 ElastiCache 복제 그룹에 대한 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

리소스 유형: AWS::ElastiCache::ReplicationGroup

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticache-repl-grp-redis-auth-enabled

Amazon ElastiCache 복제 그룹에 Redis 인증이 활성화되어 있는지 확인합니다. 해당 노드의 Redis 버전이 6 이하(버전 6 이상은 Redis ACL 사용)이고 'AuthToken'이 없거나, 비어 있거나/null인 경우 ElastiCache 복제 그룹에 대한 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

리소스 유형: AWS::ElastiCache::ReplicationGroup

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticache-subnet-group-check

Amazon ElastiCache 클러스터가 사용자 지정 서브넷 그룹으로 구성되어 있는지 확인합니다. 기본 서브넷 그룹을 사용하는 ElastiCache 클러스터에 대한 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICACHE_SUBNET_GROUP_CHECK

리소스 유형: AWS::ElastiCache::CacheCluster

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticache-supported-engine-version

ElastiCache 클러스터가 권장 엔진 버전 이상이거나 같은 버전을 실행하고 있는지 확인합니다. ElastiCache 클러스터의 'EngineVersion'이 해당 엔진에 대해 지정된 권장 버전보다 낮은 버전인 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICACHE_SUPPORTED_ENGINE_VERSION

리소스 유형: AWS::ElastiCache::CacheCluster

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

latestMemcachedVersion, 유형: 문자열

Memcached에 권장되는 최신 엔진 버전입니다. 유효한 값은 메이저, 마이너, 패치 버전을 나타내는 3자리 구성 요소 숫자로 된 의미 체계 버전 관리(SemVer) 형식입니다(예: 1.6이 아닌 1.6.6).

latestRedisVersion, 유형: 문자열

Redis에 권장되는 최신 엔진 버전입니다. 유효한 값은 메이저, 마이너, 패치 버전을 나타내는 3자리 구성 요소 숫자로 된 의미 체계 버전 관리(SemVer) 형식입니다(예: 7.0이 아닌 7.0.5).

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticbeanstalk-application-description

AWS Elastic Beanstalk 애플리케이션에 설명이 있는지 확인합니다. configuration.description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICBEANSTALK_APPLICATION_DESCRIPTION

리소스 유형: AWS::ElasticBeanstalk::Application

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticbeanstalk-application-version-description

AWS Elastic Beanstalk 애플리케이션 버전에 설명이 있는지 확인합니다. configuration.description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICBEANSTALK_APPLICATION_VERSION_DESCRIPTION

리소스 유형: AWS::ElasticBeanstalk::ApplicationVersion

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticbeanstalk-environment-description

AWS Elastic Beanstalk 환경에 설명이 있는지 확인합니다. configuration.description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICBEANSTALK_ENVIRONMENT_DESCRIPTION

리소스 유형: AWS::ElasticBeanstalk::Environment

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticsearch-encrypted-at-rest

Amazon OpenSearch Service(이전 이름 Elasticsearch) 도메인에 저장 시 암호화 구성이 활성화되어 있는지 확인합니다. EncryptionAtRestOptions 필드가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICSEARCH_ENCRYPTED_AT_REST

리소스 유형: AWS::Elasticsearch::Domain

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticsearch-in-vpc-only

Amazon OpenSearch Service(이전 이름 Elasticsearch)가 Amazon Virtual Private Cloud(VPC)에 있는지 확인합니다. OpenSearch Service 도메인 엔드포인트가 퍼블릭이면 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICSEARCH_IN_VPC_ONLY

리소스 유형: AWS::Elasticsearch::Domain

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticsearch-logs-to-cloudwatch

Amazon CloudWatch Logs에 로그를 전송하도록 Amazon OpenSearch Service 도메인이 구성되어 있는지 확인합니다. Amazon ES 도메인에 대한 로그가 활성화된 경우 규칙은 COMPLIANT입니다. 로깅이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICSEARCH_LOGS_TO_CLOUDWATCH

리소스 유형: AWS::Elasticsearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

logTypes(선택 사항), 유형: CSV

활성화된 로그를 쉼표로 구분한 목록입니다. 유효한 값은 'search', 'index', 'error'입니다.

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
   "LogPublishingOptions": "{Key : Value, ...}"*
}
...
```

*게시하려는 로그 유형에 따라 `SEARCH_SLOW_LOGS`, `ES_APPLICATION_LOGS`, `INDEX_SLOW_LOGS`, `AUDIT_LOGS` 키가 하나 이상 있는 객체입니다. 각 키에는 유효한 `LogPublishingOption` 값이 필요합니다.

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elasticsearch-node-to-node-encryption-check

OpenSearch Service(이전 이름 Elasticsearch) 노드가 처음부터 끝까지 암호화되어 있는지 확인합니다. 도메인에서 노드 간 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

리소스 유형: AWS::Elasticsearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
   "NodeToNodeEncryptionOptions": BOOLEAN
}
...
```

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elastic-beanstalk-logs-to-cloudwatch

AWS Elastic Beanstalk 환경이 Amazon CloudWatch Logs로 로그를 전송하도록 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH

리소스 유형: AWS::ElasticBeanstalk::Environment

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

RetentionInDays(선택 사항), 유형: 문자열

> 만료 전 로그 이벤트를 유지할 일수를 확인합니다. 유효한 값은 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, 3653입니다. 'logs.RetentionInDays' 값이 이 파라미터와 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

DeleteOnTerminate(선택 사항), 유형: 문자열

> 환경 종료 시 로그를 삭제하도록 구성되어 있는지 확인합니다. 유효한 값은 'true' 또는 'false'입니다. 'logs.DeleteOnTerminate' 값이 이 파라미터와 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elastic-beanstalk-managed-updates-enabled

AWS Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트가 활성화되어 있는지 확인합니다. 값이 `ManagedActionsEnabled`로 설정된 경우 규칙은 COMPLIANT입니다. `ManagedActionsEnabled`의 값이 false로 설정되어 있거나, 값이 기존 구성과 일치하지 않는 파라미터가 제공된 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

리소스 유형: AWS::ElasticBeanstalk::Environment

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

UpdateLevel(선택 사항), 유형: 문자열

업데이트 수준이 '마이너' 버전 업데이트로 설정되어 있는지 또는 '패치' 버전 업데이트로 설정되어 있는지 나타냅니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elbv2-acm-certificate-required

Application Load Balancer 및 Network Load Balancer에 AWS Certificate Manager (ACM)의 인증서를 사용하도록 구성된 리스너가 있는지 확인합니다. ACM의 인증서 없이 구성되었거나, ACM의 인증서와 다른 인증서로 구성된 하나 이상의 리스너가 하나 이상의 로드 밸런서에 있는 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: ELBV2_ACM_CERTIFICATE_REQUIRED

리소스 유형: AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

AcmCertificatesAllowed(선택 사항), 유형: CSV

인증서 Amazon 리소스 이름(ARN)을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

전송 중 elbv2-listener-encryption-in-transit

로드 밸런서의 리스너가 HTTPS 또는 TLS 종료로 구성되어 있는지 확인합니다. 리스너가 HTTPS 또는 TLS 종료로 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELBV2_LISTENER_ENCRYPTION_IN_TRANSIT

리소스 유형: AWS::ElasticLoadBalancingV2::Listener

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(서울), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elbv2-multiple-az

Elastic Load Balancer V2(Application, Network 또는 Gateway Load Balancer)가 여러 가용 영역(AZ)에 매핑되어 있는지 확인합니다. Elastic Load Balancer V2가 2개 이하의 AZ에 매핑되어 있는 경우 규칙은 NON_COMPLIANT입니다. 자세한 내용은 Application Load Balancer 가용 영역을 참조하세요.

식별자: ELBV2_MULTIPLE_AZ

리소스 유형: AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

minAvailabilityZones(선택 사항), 유형: int

최소 예상 AZ 수(2~10개 사이)

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elbv2-predefined-security-policy-ssl-check

Application Load Balancer(ALBs) 또는 Network Load Balancer(NLBs)의 리스너가 특정 보안 정책을 사용하는지 확인합니다. ALB의 HTTPS 리스너 또는 NLB의 TLS 리스너가 지정한 보안 정책을 사용하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELBV2_PREDEFINED_SECURITY_POLICY_SSL_CHECK

리소스 유형: AWS::ElasticLoadBalancingV2::Listener

트리거 0유형: 구성 변경

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

sslPolicies, 유형: CSV

확인할 규칙에 대한 SSL 보안 정책의 쉼표로 구분된 목록입니다. 예: "ELBSecurityPolicy-TLS13-1-2-2021-06".

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elb-acm-certificate-required

Classic Load Balancer가에서 제공하는 SSL 인증서를 사용하는지 확인합니다 AWS Certificate Manager. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다.

이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

식별자: ELB_ACM_CERTIFICATE_REQUIRED

리소스 유형: AWS::ElasticLoadBalancing::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 아프리카(케이프타운), 아시아 태평양(오사카), 유럽(밀라노), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elb-cross-zone-load-balancing-enabled

Classic Load Balancer에 대해 교차 영역 로드 밸런싱이 활성화되었는지 확인합니다. Classic Load Balancer에 대해 교차 영역 로드 밸런싱이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

리소스 유형: AWS::ElasticLoadBalancing::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elb-custom-security-policy-ssl-check

Classic Load Balancer SSL 리스너가 사용자 지정 정책을 사용하고 있는지 확인합니다. Classic Load Balancer에 대한 SSL 리스너가 있는 경우에만 규칙이 적용됩니다.

식별자: ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

리소스 유형: AWS::ElasticLoadBalancing::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(자카르타), 아시아 태평양(오사카), 아시아 태평양(멜버른), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

sslProtocolsAndCiphers, 유형: 문자열

암호와 프로토콜을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elb-deletion-protection-enabled

Elastic Load Balancer의 삭제 방지 기능이 활성화되었는지 확인합니다. deletion_protection.enabled가 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELB_DELETION_PROTECTION_ENABLED

리소스 유형: AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(오사카) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elb-logging-enabled

Application Load Balancer 및 Classic Load Balancer에 로깅이 활성화되어 있는지 확인합니다. `access_logs.s3.enabled`가 false이거나 `access_logs.S3.bucket`이 사용자가 지정한 s3BucketName과 다른 경우 규칙이 NON_COMPLIANT로 간주됩니다.

> **Note**
>
> 이 규칙은 Network Load Balancer 또는 Gateway Load Balancer에는 적용되지 않습니다.

식별자: ELB_LOGGING_ENABLED

리소스 유형: AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

s3BucketNames(선택 사항), 유형: CSV

로그 파일을 전송하기 위한 Amazon ELB용 Amazon S3 버킷 이름을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elb-predefined-security-policy-ssl-check

Classic Load Balancer SSL 리스너가 미리 정의된 정책을 사용하는지 확인합니다. Classic Load Balancer HTTPS/SSL 리스너의 정책이 '`predefinedPolicyName`' 파라미터의 값과 같지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

리소스 유형: AWS::ElasticLoadBalancing::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(오사카) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

predefinedPolicyName, 유형: 문자열

사전 정의된 정책의 이름입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

elb-tls-https-listeners-only

Classic Load Balancer가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인합니다. 리스너가 SSL 또는 HTTPS로 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

- Classic Load Balancer에 리스너가 구성되어 있지 않으면 규칙이를 반환합니다`NOT_APPLICABLE`.
- Classic Load Balancer 리스너가 SSL 또는 HTTPS로 구성되어 있는 경우 규칙은 COMPLIANT입니다.
- 리스너가 SSL 또는 HTTPS로 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: ELB_TLS_HTTPS_LISTENERS_ONLY

리소스 유형: AWS::ElasticLoadBalancing::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 중동(UAE), 아시아 태평양(오사카) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

emr-block-public-access

Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

식별자: EMR_BLOCK_PUBLIC_ACCESS

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

emr-kerberos-enabled

Amazon EMR 클러스터에 Kerberos가 활성화되어 있는지 확인합니다. 보안 구성이 클러스터에 연결되어 있지 않거나 보안 구성이 지정된 규칙 파라미터를 충족하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: EMR_KERBEROS_ENABLED

리소스 유형: AWS::EMR::Cluster

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

TicketLifetimeInHours(선택 사항), 유형: int

클러스터의 KDC에서 발행한 Kerberos 티켓이 유효한 기간입니다.

Realm(선택 사항), 유형: 문자열

신뢰 관계에 있는 다른 영역의 Kerberos 영역 이름입니다.

Domain(선택 사항), 유형: 문자열

신뢰 관계에 있는 다른 영역의 도메인 이름입니다.

AdminServer(선택 사항), 유형: 문자열

신뢰 관계의 다른 영역에 있는 관리 서버의 정규화된 도메인입니다.

KdcServer(선택 사항), 유형: 문자열

신뢰 관계의 다른 영역에 있는 KDC 서버의 정규화된 도메인입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

emr-master-no-public-ip

Amazon EMR 클러스터의 마스터 노드에 퍼블릭 IP가 있는지 확인합니다. 마스터 노드에 퍼블릭 IP가 있으면 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 이 규칙은 RUNNING 또는 WAITING 상태에 있는 클러스터를 확인합니다. 이 규칙을 사용하여 정확한 평가를 하려면 `AWS::EC2::Instance` 리소스 유형에 대한 기록을 활성화해야 합니다.

식별자: EMR_MASTER_NO_PUBLIC_IP

리소스 유형: AWS::EMR::Cluster, AWS::EC2::Instance

트리거 유형: 주기적

AWS 리전: 아시아 태평양(오사카), 아시아 태평양(멜버른), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

emr-security-configuration-encryption-rest

Amazon EMR 보안 구성에 저장 시 암호화가 활성화되어 있는지 확인합니다. configuration.SecurityConfiguration.EncryptionConfiguration.EnableAtRestEncryption이 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: EMR_SECURITY_CONFIGURATION_ENCRYPTION_REST

리소스 유형: AWS::EMR::SecurityConfiguration

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

emr-security-configuration-encryption-transit

Amazon EMR 보안 구성에 전송 중 암호화가 활성화되어 있는지 확인합니다. configuration.SecurityConfiguration.EncryptionConfiguration.EnableInTransitEncryption이 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: EMR_SECURITY_CONFIGURATION_ENCRYPTION_TRANSIT

리소스 유형: AWS::EMR::SecurityConfiguration

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

encrypted-volumes

연결된 Amazon EBS 볼륨이 암호화되어 있고, 선택에 따라 지정된 KMS 키로 암호화되어 있는지 확인합니다. 연결된 EBS 볼륨이 암호화되지 않았거나, 제공된 파라미터에 없는 KMS 키로 암호화된 경우 규칙은 NON_COMPLIANT입니다.

식별자: ENCRYPTED_VOLUMES

리소스 유형: AWS::EC2::Volume

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

kmsId(선택 사항), 유형: 문자열

볼륨 암호화에 사용되는 KMS 키의 ID 또는 ARN입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

event-data-store-cmk-encryption-enabled

AWS Cloud Trail 이벤트 데이터 스토어에 고객 관리형 AWS KMS 키가 활성화되어 있는지 확인합니다. 이벤트 데이터 스토어가 고객 관리형 KMS 키를 비활성화한 경우 규칙은 NON_COMPLIANT입니다. 선택적으로 확인할 규칙에 대한 KMS 키 목록을 지정할 수 있습니다.

식별자: EVENT_DATA_STORE_CMK_ENCRYPTION_ENABLED

리소스 유형: AWS::CloudTrail::EventDataStore

트리거 유형: 주기적

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: CSV

> 확인할 규칙에 대한 AWS KMS 키의 Amazon 리소스 이름(ARNs)을 쉼표로 구분한 목록입니다. 제공된 경우 AWS Cloud Trail 이벤트 데이터 스토어가 이러한 KMS 키 중 하나로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

evidently-launch-description

Amazon CloudWatch Evidently 시작에 설명이 있는지 확인합니다. configuration.Description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: EVIDENTLY_LAUNCH_DESCRIPTION

리소스 유형: AWS::Evidently::Launch

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

evidently-launch-tagged

Amazon CloudWatch Evidently 시작에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EVIDENTLY_LAUNCH_TAGGED

리소스 유형: AWS::Evidently::Launch

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

evidently-project-description

Amazon CloudWatch Evidently 프로젝트에 설명이 있는지 확인합니다. configuration.Description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: EVIDENTLY_PROJECT_DESCRIPTION

리소스 유형: AWS::Evidently::Project

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

evidently-project-tagged

Amazon CloudWatch Evidently 프로젝트에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EVIDENTLY_PROJECT_TAGGED

리소스 유형: AWS::Evidently::Project

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

evidently-segment-description

Amazon CloudWatch Evidently 세그먼트에 설명이 있는지 확인합니다. configuration.Description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: EVIDENTLY_SEGMENT_DESCRIPTION

리소스 유형: AWS::Evidently::Segment

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

evidently-segment-tagged

Amazon CloudWatch Evidently 세그먼트에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: EVIDENTLY_SEGMENT_TAGGED

리소스 유형: AWS::Evidently::Segment

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fis-experiment-template-log-configuration-exists

AWS FIS 실험 템플릿에 실험 로깅이 구성되어 있는지 확인합니다. configuration.LogConfiguration이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: FIS_EXPERIMENT_TEMPLATE_LOG_CONFIGURATION_EXISTS

리소스 유형: AWS::FIS::ExperimentTemplate

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fis-experiment-template-tagged

AWS FIS 실험 템플릿에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: FIS_EXPERIMENT_TEMPLATE_TAGGED

리소스 유형: AWS::FIS::ExperimentTemplate

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fms-shield-resource-policy-check

AWS Shield Advanced가 보호할 수 있는 리소스가 Shield Advanced에 의해 보호되는지 확인합니다. 지정된 리소스가 보호되지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: FMS_SHIELD_RESOURCE_POLICY_CHECK

리소스 유형: AWS::CloudFront::Distribution, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::WAFRegional::WebACL, AWS::EC2::EIP, AWS::ElasticLoadBalancing::LoadBalancer, AWS::ShieldRegional::Protection, AWS::Shield::Protection

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(말레이시아), 멕시코(중부), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

webACLId, 유형: 문자열

웹 ACL의 고유 식별자입니다.

resourceTypes, 유형: 문자열

확인할 규칙에 대해 지정하는 리소스 유형입니다.

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대해 지정하는 리소스 태그입니다. 예: { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }.

excludeResourceTags(선택 사항), 유형: boolean

true인 경우 규칙은 resourceTags. false인 경우 규칙에는 resourceTags에 지정된 모든 리소스가 포함됩니다.

fmsManagedToken(선택 사항), 유형: 문자열

계정에서 규칙을 생성할 때 AWS Firewall Manager에서 생성한 토큰. AWS Config는이 규칙을 생성할 때이 파라미터를 무시합니다.

fmsRemediationEnabled(선택 사항), 유형: boolean

true인 경우 AWS Firewall Manager는 FMS 정책에 따라 NON_COMPLIANT 리소스를 업데이트합니다.이 규칙을 생성할 때 AWS 구성은이 파라미터를 무시합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fms-webacl-resource-policy-check

웹 ACL이 Application Load Balancer, API 게이트웨이 단계 또는 Amazon CloudFront 배포와 연결되어 있는지 확인합니다. 에서이 규칙을 AWS Firewall Manager 생성할 때 FMS 정책 소유자는 FMS 정책에 `WebACLId`를 지정하고 선택적으로 문제 해결을 활성화할 수 있습니다.

식별자: FMS_WEBACL_RESOURCE_POLICY_CHECK

리소스 유형: AWS::CloudFront::Distribution, AWS::ApiGateway::Stage, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::WAFRegional::WebACL

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

webACLId, 유형: 문자열

웹 ACL의 WebACLId입니다.

resourceTags(선택 사항), 유형: 문자열

규칙을 연결해야 하는 리소스 태그(ApplicationLoadBalancer, ApiGatewayStage 및 CloudFront distributions)입니다(예: { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }).

excludeResourceTags(선택 사항), 유형: boolean

true인 경우, resourceTags와 일치하는 리소스를 제외합니다.

fmsManagedToken(선택 사항), 유형: 문자열

고객 계정에서 규칙을 생성할 때 AWS Firewall Manager에서 생성한 토큰. AWS Config는 고객이이 규칙을 생성할 때이 파라미터를 무시합니다.

fmsRemediationEnabled(선택 사항), 유형: boolean

true인 경우 AWS Firewall Manager는 FMS 정책에 따라 규정 미준수 리소스를 업데이트합니다. AWS Config는 고객이이 규칙을 생성할 때이 파라미터를 무시합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fms-webacl-rulegroup-association-check

규칙 그룹이 올바른 우선순위로 웹 ACL가 연결되는지 확인합니다. 올바른 우선순위는 ruleGroups 파라미터의 규칙 그룹 순위에 따라 결정됩니다. 가이 규칙을 AWS Firewall Manager 생성하면 우선 순위

가 가장 높은 0에 이어 1, 2 등을 할당합니다. FMS 정책 소유자는 FMS 정책에 `ruleGroups` 순위를 지정하고, 필요할 경우 문제 해결을 활성화할 수 있습니다.

식별자: FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

리소스 유형: AWS::WAF::WebACL, AWS::WAFRegional::WebACL

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

ruleGroups, 유형: 문자열

RuleGroupIds와 WafOverrideAction 페어를 쉼표로 구분한 목록입니다(예: ruleGroupId-1:NONE, ruleGroupId2:COUNT).

fmsManagedToken(선택 사항), 유형: 문자열

고객 계정에서 규칙을 생성할 때 AWS Firewall Manager에서 생성한 토큰입니다. AWS Config는 고객이이 규칙을 생성할 때이 파라미터를 무시합니다.

fmsRemediationEnabled(선택 사항), 유형: boolean

true인 경우 AWS Firewall Manager는 FMS 정책에 따라 규정 미준수 리소스를 업데이트합니다. AWS Config는 고객이이 규칙을 생성할 때이 파라미터를 무시합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

frauddetector-entity-type-tagged

Amazon Fraud Detector 엔터티 유형에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: FRAUDDETECTOR_ENTITY_TYPE_TAGGED

리소스 유형: AWS::FraudDetector::EntityType

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(오하이오), 유럽(아일랜드), 미국 동부(버지니아 북부), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

frauddetector-label-tagged

Amazon Fraud Detector 레이블에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: FRAUDDETECTOR_LABEL_TAGGED

리소스 유형: AWS::FraudDetector::Label

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(오하이오), 유럽(아일랜드), 미국 동부(버지니아 북부), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

frauddetector-outcome-tagged

Amazon Fraud Detector 결과에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: FRAUDDETECTOR_OUTCOME_TAGGED

리소스 유형: AWS::FraudDetector::Outcome

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(오하이오), 유럽(아일랜드), 미국 동부(버지니아 북부), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

frauddetector-variable-tagged

Amazon Fraud Detector 변수에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: FRAUDDETECTOR_VARIABLE_TAGGED

리소스 유형: AWS::FraudDetector::Variable

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(오하이오), 유럽(아일랜드), 미국 동부(버지니아 북부), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fsx-last-backup-recovery-point-created

Amazon FSx 파일 시스템에 대한 복구 시점이 생성되었는지 확인합니다. 지정된 기간 내에 생성된 해당하는 복구 시점이 Amazon FSx 파일 시스템에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: FSX_LAST_BACKUP_RECOVERY_POINT_CREATED

리소스 유형: AWS::FSx::FileSystem

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

> 확인할 규칙에 대한 Amazon FSx 파일 시스템의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

> 확인할 규칙에 대한 Amazon FSx 파일 시스템의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 744시간, 일수는 31일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fsx-lustre-copy-tags-to-backups

Amazon FSX for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있는지 확인합니다. Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: FSX_LUSTRE_COPY_TAGS_TO_BACKUPS

리소스 유형: AWS::FSx::FileSystem

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fsx-meets-restore-time-target

Amazon FSx 파일 시스템의 복원 시간이 지정된 기간을 충족하는지 확인합니다. Amazon FSx 파일 시스템의 LatestRestoreExecutionTimeMinutes가 maxRestoreTime(분)보다 큰 경우 규칙은 NON_COMPLIANT입니다.

식별자: FSX_MEETS_RESTORE_TIME_TARGET

리소스 유형: AWS::FSx::FileSystem

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

maxRestoreTime, 유형: int

허용되는 최대 복원 런타임의 숫자 값입니다.

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon FSx 파일 시스템의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon FSx 파일 시스템의 ID입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fsx-ontap-deployment-type-check

Amazon FSx for NetApp ONTAP 파일 시스템이 특정 배포 유형으로 구성되어 있는지 확인합니다. Amazon FSx for NetApp ONTAP 파일 시스템이 지정한 배포 유형으로 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: FSX_ONTAP_DEPLOYMENT_TYPE_CHECK

리소스 유형: AWS::FSx::FileSystem

트리거 유형: 주기적

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

deploymentTypes, 유형: CSV

확인할 규칙에 허용되는 배포 유형의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fsx-openzfs-copy-tags-enabled

Amazon FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있는지 확인합니다. FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: FSX_OPENZFS_COPY_TAGS_ENABLED

리소스 유형: AWS::FSx::FileSystem

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fsx-openzfs-deployment-type-check

Amazon FSx for OpenZFS 파일 시스템이 특정 배포 유형으로 구성되어 있는지 확인합니다. FSx for OpenZFS 파일 시스템이 지정한 배포 유형으로 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: FSX_OPENZFS_DEPLOYMENT_TYPE_CHECK

리소스 유형: AWS::FSx::FileSystem

트리거 유형: 주기적

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

deploymentTypes, 유형: CSV

확인할 규칙에 허용되는 배포 유형의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fsx-resources-protected-by-backup-plan

Amazon FSx 파일 시스템이 백업 계획에 의해 보호되고 있는지 확인합니다. Amazon FSx 파일 시스템을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN

리소스 유형: AWS::FSx::FileSystem

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon FSx 파일 시스템의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon FSx 파일 시스템의 ID입니다.

crossRegionList(선택 사항), 유형: 문자열

리전 간 백업 사본을 보관할 대상 리전을 쉼표로 구분한 목록입니다.

crossAccountList(선택 사항), 유형: 문자열

계정 간 백업 사본을 보관할 대상 계정을 쉼표로 구분한 목록입니다.

maxRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최대 보존 기간(일)

minRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최소 보존 기간(일)

backupVaultLockCheck(선택 사항), 유형: 문자열

허용되는 값: 'True' 또는 'False'. 리소스가 잠긴 볼트에 백업되어 있는지 확인하는 규칙에 'True'를 입력합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fsx-windows-audit-log-configured

Amazon FSx for Windows File Server 파일 시스템에 파일 액세스 감사가 활성화되어 있는지 확인합니다. FSx for Windows File Server 파일 시스템에 파일 액세스 감사가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: FSX_WINDOWS_AUDIT_LOG_CONFIGURED

리소스 유형: AWS::FSx::FileSystem

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

fsx-windows-deployment-type-check

Amazon FSx for WINDOWS 파일 시스템이 특정 배포 유형으로 구성되어 있는지 확인합니다. FSx for WINDOWS 파일 시스템이 지정한 배포 유형으로 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: FSX_WINDOWS_DEPLOYMENT_TYPE_CHECK

리소스 유형: AWS::FSx::FileSystem

트리거 유형: 주기적

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 유럽(파리), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

deploymentTypes, 유형: CSV

확인할 규칙에 허용되는 배포 유형의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

glb-listener-tagged

Gateway Load Balancer 리스너에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: GLB_LISTENER_TAGGED

리소스 유형: AWS::ElasticLoadBalancingV2::Listener

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

global-endpoint-event-replication-enabled

Amazon EventBridge 글로벌 엔드포인트에 대해 이벤트 복제가 활성화되어 있는지 확인합니다. 이벤트 복제가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: GLOBAL_ENDPOINT_EVENT_REPLICATION_ENABLED

리소스 유형: AWS::Events::Endpoint

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(오사카), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

glue-job-logging-enabled

AWS Glue 작업에 로깅이 활성화되어 있는지 확인합니다. AWS Glue 작업에 Amazon CloudWatch logs가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: GLUE_JOB_LOGGING_ENABLED

리소스 유형: AWS::Glue::Job

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

glue-ml-transform-encrypted-at-rest

AWS Glue ML 변환에 저장 시 암호화가 활성화되어 있는지 확인합니다. `MLUserDataEncryptionMode`가 `DISABLED`로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: GLUE_ML_TRANSFORM_ENCRYPTED_AT_REST

리소스 유형: AWS::Glue::MLTransform

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

glue-spark-job-supported-version

AWS Glue Spark 작업이 지정된 지원되는 최소 AWS Glue 버전에서 실행 중인지 확인합니다. 지정한 지원되는 최소 Glue 버전에서 AWS AWS Glue Spark 작업이 실행되지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: GLUE_SPARK_JOB_SUPPORTED_VERSION

리소스 유형: AWS::Glue::Job

트리거 0유형: 구성 변경

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

minimumSupportedGlueVersion, 유형: 문자열

확인할 규칙에 대해 지원되는 최소 AWS Glue 버전의 문자열 값을 지정해야 합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

guardduty-ec2-protection-runtime-enabled

Amazon GuardDuty 감지기에 대해 자동 에이전트 관리를 사용한 ECS 런타임 모니터링이 활성화되어 있는지 확인합니다. 사용자 계정 또는 조직의 하나 이상의 멤버 계정에 대해 기능이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: GUARDDUTY_EC2_PROTECTION_RUNTIME_ENABLED

리소스 유형: AWS::GuardDuty::Detector

트리거 유형: 주기적

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

guardduty-ecs-protection-runtime-enabled

Amazon GuardDuty 감지기에 대해 자동 에이전트 관리를 사용한 ECS 런타임 모니터링이 활성화되어 있는지 확인합니다. 사용자 계정 또는 조직의 하나 이상의 멤버 계정에 대해 기능이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: GUARDDUTY_ECS_PROTECTION_RUNTIME_ENABLED

리소스 유형: AWS::GuardDuty::Detector

트리거 유형: 주기적

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

guardduty-eks-protection-audit-enabled

계정의 Amazon GuardDuty 탐지기에 대해 Amazon Elastic Kubernetes Service(Amazon EKS)에 대한 감사 로그 모니터링이 활성화되어 있는지 확인합니다. 계정에 대해 EKS 감사 로그 모니터링 기능이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: GUARDDUTY_EKS_PROTECTION_AUDIT_ENABLED

리소스 유형: AWS::GuardDuty::Detector

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

guardduty-eks-protection-runtime-enabled

계정의 GuardDuty 탐지기에 대해 자동 에이전트 관리를 사용한 Amazon EKS 런타임 모니터링이 활성화되어 있는지 확인합니다. GuardDuty에서 자동 에이전트 관리를 사용한 EKS 런타임 모니터링이 계정에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: GUARDDUTY_EKS_PROTECTION_RUNTIME_ENABLED

리소스 유형: AWS::GuardDuty::Detector

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

guardduty-enabled-centralized

AWS 계정 및 AWS 리전에서 Amazon GuardDuty가 활성화되어 있는지 확인합니다. 중앙 집중화를 위한 AWS 계정을 제공하는 경우 규칙은 중앙 집중식 계정의 GuardDuty 결과를 평가합니다. GuardDuty가 활성화되어 있을 경우 규칙은 COMPLIANT입니다.

식별자: GUARDDUTY_ENABLED_CENTRALIZED

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

CentralMonitoringAccount(선택 사항), 유형: 문자열

Amazon GuardDuty 결과를 중앙 집중화할 수 있는 쉼표로 구분된 AWS 계정 목록(12자리).

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

guardduty-lambda-protection-enabled

계정의 Amazon GuardDuty 감지기에 대해 Lambda 보호가 활성화되어 있는지 확인합니다. Amazon GuardDuty의 Lambda 보호 기능이 계정에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: GUARDDUTY_LAMBDA_PROTECTION_ENABLED

리소스 유형: AWS::GuardDuty::Detector

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

guardduty-malware-protection-enabled

계정의 Amazon GuardDuty 탐지기에 대해 맬웨어 보호가 활성화되어 있는지 확인합니다. Amazon GuardDuty의 맬웨어 보호 기능이 계정에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: GUARDDUTY_MALWARE_PROTECTION_ENABLED

리소스 유형: AWS::GuardDuty::Detector

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

guardduty-non-archived-findings

Amazon GuardDuty에 보관되지 않은 결과가 있는지 확인합니다. daysLowSev/daysMediumSev/`daysHighSev` 파라미터에 지정된 일수보다 오랫동안 보관되지 않은 낮은/중간/높은 심각도의 결과가 GuardDuty에 있을 경우 규칙은 NON_COMPLIANT입니다.

식별자: GUARDDUTY_NON_ARCHIVED_FINDINGS

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

daysLowSev(선택 사항), 유형: int, 기본값: 30

Amazon GuardDuty의 낮은 심각도 결과가 보관되지 않은 상태로 유지될 수 있는 일수입니다. 기본값은 30일입니다.

daysMediumSev(선택 사항), 유형: int, 기본값: 7

Amazon GuardDuty의 중간 심각도 결과가 보관되지 않은 상태로 유지될 수 있는 일수입니다. 기본값은 7일입니다.

daysHighSev(선택 사항), 유형: int, 기본값: 1

Amazon GuardDuty의 높은 심각도 결과가 보관되지 않은 상태로 유지될 수 있는 일수입니다. 기본값은 1일입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

guardduty-rds-protection-enabled

계정의 Amazon GuardDuty 탐지기에 대해 Amazon Relational Database Service(Amazon RDS) 보호가 활성화되어 있는지 확인합니다. Amazon GuardDuty의 Amazon RDS 보호 기능이 계정에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: GUARDDUTY_RDS_PROTECTION_ENABLED

리소스 유형: AWS::GuardDuty::Detector

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

guardduty-runtime-monitoring-enabled

계정 또는 조직의 Amazon GuardDuty 감지기에 대해 런타임 모니터링이 활성화되어 있는지 확인합니다. GuardDuty의 런타임 모니터링이 계정 또는 조직의 하나 이상의 멤버 계정에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: GUARDDUTY_RUNTIME_MONITORING_ENABLED

리소스 유형: AWS::GuardDuty::Detector

트리거 유형: 주기적

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

guardduty-s3-protection-enabled

계정의 Amazon GuardDuty 감지기에 대해 S3 보호가 활성화되어 있는지 확인합니다. Amazon GuardDuty의 S3 보호 기능이 계정에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: GUARDDUTY_S3_PROTECTION_ENABLED

리소스 유형: AWS::GuardDuty::Detector

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-customer-policy-blocked-kms-actions

생성한 관리형 AWS Identity and Access Management(IAM) 정책이 모든 KMS 키 리소스에서 차단된 AWS KMS 작업을 허용하지 않는지 확인합니다. 관리형 IAM 정책에서 모든 AWS KMS 키에 대해 차단된 작업이 허용되는 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 비공개로 간주되려면 IAM 정책이 고정 값에 대한 액세스 권한만 부여해야 합니다. 즉, 와일드카드 또는 변수라는 IAM 정책 요소가 포함되지 않은 값을 의미합니다https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_variables.html#policy-vars-using-variables.

식별자: IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

리소스 유형: AWS::IAM::Policy

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

blockedActionsPatterns, 유형: CSV

확인할 규칙에 대해 차단된 KMS 작업 패턴의 쉼표로 구분된 목록입니다. IAM 고객 관리형 정책이 지정한 작업에 대한 모든 리소스에 와일드카드 액세스를 허용하는 경우 규칙은 NON_COMPLIANT 입니다.

excludePermissionBoundaryPolicy(선택 사항), 유형: boolean

권한 경계로 사용되는 IAM 정책의 평가를 제외하기 위한 부울 플래그입니다. 'true'로 설정하면 규칙은 평가 시 권한 경계를 포함하지 않습니다. 그렇지 않을 경우 값이 'false'로 설정되면 범위 내의 모든 IAM 정책이 평가됩니다. 기본값은 'false'입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-external-access-analyzer-enabled

리전별 계정에서 외부 액세스용 IAM Access Analyzer가 활성화되었는지 확인합니다. 리전에 외부 액세스를 위한 분석기가 없거나 '상태' 속성이 '활성'으로 설정되지 않은 경우 규칙은 NON_COMPLIANT 입니다.

식별자: IAM_EXTERNAL_ACCESS_ANALYZER_ENABLED

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-group-has-users-check

IAM 그룹에 IAM 사용자가 한 명 이상 존재하는지 확인합니다.

식별자: IAM_GROUP_HAS_USERS_CHECK

리소스 유형: AWS::IAM::Group

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-inline-policy-blocked-kms-actions

IAM 사용자, 역할 및 그룹에 연결된 인라인 정책이 모든 AWS KMS 키에 대해 차단된 작업을 허용하지 않는지 확인합니다. 인라인 정책의 모든 AWS KMS 키에 대해 차단된 작업이 허용되는 경우 규칙은 NON_COMPLIANT입니다.

식별자: IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

리소스 유형: AWS::IAM::Group, AWS::IAM::Role, AWS::IAM::User

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

blockedActionsPatterns, 유형: CSV

차단된 KMS 작업 패턴을 쉼표로 구분한 목록입니다(예: kms:*, kms:Decrypt, kms:ReEncrypt*).

excludeRoleByManagementAccount(선택 사항), 유형: boolean

조직 관리 계정에서만 수임 가능한 역할인 경우 해당 역할을 제외합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-no-inline-policy-check

인라인 정책 기능이 사용 중이 아닌지 확인합니다. AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 인라인 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: IAM_NO_INLINE_POLICY_CHECK

리소스 유형: AWS::IAM::User, AWS::IAM::Role, AWS::IAM::Group

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-oidc-provider-tagged

AWS IAM OIDC 공급자에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IAM_OIDC_PROVIDER_TAGGED

리소스 유형: AWS::IAM::OIDCProvider

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-password-policy

AWS Identity and Access Management(IAM) 사용자의 계정 암호 정책이 파라미터에 표시된 지정된 요구 사항을 충족하는지 확인합니다. 계정 암호 정책이 지정된 요구 사항을 충족하지 않는 경우 규칙은 NON_COMPLIANT입니다.

> **Important**
>
> 규칙 파라미터의 `true` 및 `false` 값은 대소문자를 구분합니다. `true`를 소문자로 입력하지 않으면 `false.`로 처리됩니다.

> **Note**
>
> 기본 IAM 암호 정책에 대한 평가 결과
> 기본 IAM 암호 정책을 사용하는 경우 이 규칙은 NON-COMPLIANT로 표시됩니다.
> 관리형 규칙 및 글로벌 IAM 리소스 유형
> 2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사

용 가능한 AWS 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 리소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에서는 기록할 수 없습니다. 해당 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.
주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.
불필요한 평가를 방지하려면 지원되는 리전 중 하나에만 글로벌 IAM 리소스 유형에 대해 규정 준수를 보고하는 주기적 규칙을 배포해야 합니다. 리전에서 지원되는 관리형 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.

식별자: IAM_PASSWORD_POLICY

트리거 유형: 주기적

AWS 리전: 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

RequireUppercaseCharacters(선택 사항), 유형: boolean, 기본값: true

암호에 대문자가 한 개 이상이어야 합니다.

RequireLowercaseCharacters(선택 사항), 유형: boolean, 기본값: true

암호에 소문자가 한 개 이상이어야 합니다.

RequireSymbols(선택 사항), 유형: boolean, 기본값: true

암호에 기호가 한 개 이상이어야 합니다.

RequireNumbers(선택 사항), 유형: boolean, 기본값: true

암호에 숫자가 한 개 이상이어야 합니다.

MinimumPasswordLength(선택 사항), 유형: int, 기본값: 14

암호 최소 길이입니다.

PasswordReusePrevention(선택 사항), 유형: int, 기본값: 24

재사용을 허가받기까지 사용할 수 있는 암호 개수입니다.

MaxPasswordAge(선택 사항), 유형: int, 기본값: 90

암호 만료까지 남은 일수입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-policy-blacklisted-check

입력 파라미터의 정책 Amazon 리소스 이름(ARN)이 IAM 리소스에 연결되어 있는지 각 AWS Identity and Access Management(IAM) 리소스를 확인합니다. 정책 ARN이 IAM 리소스에 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: IAM_POLICY_BLACKLISTED_CHECK

리소스 유형: AWS::IAM::User, AWS::IAM::Group, AWS::IAM::Role

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

policyArns, 유형: CSV, 기본값: arn:aws:iam::aws:policy/AdministratorAccess

IAM 엔터티에 연결해서는 안 되는 IAM 정책 ARN를 쉼표로 구분한 목록입니다.

exceptionList(선택 사항), 유형: CSV

쉼표로 구분된 리소스 유형 목록 및 리소스 이름 페어 목록 예를 들어, 사용자:[user1;user2], 그룹:[group1;group2], 역할:[role1;role2;role3].

> **Note**
> 예외 목록에서 전체 ARN이 아닌 리소스의 이름을 지정합니다. 유효하지 않음: `arn:aws:iam::444455556666:role/Admin` 유효함: `Admin`

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-policy-in-use

IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.

> **Note**
>
> 관리형 규칙 및 글로벌 IAM 리소스 유형
> 2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사용 가능한 AWS 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 리소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에 기록할 수 없습니다. 해당 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.
> 주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.
> 불필요한 평가를 방지하려면 지원되는 리전 중 하나에만 글로벌 IAM 리소스 유형에 대해 규정 준수를 보고하는 주기적 규칙을 배포해야 합니다. 리전에서 지원되는 관리형 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.

식별자: IAM_POLICY_IN_USE

리소스 유형: AWS::IAM::Policy

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

policyARN, 유형: 문자열

IAM 정책 ARN을 확인해야 합니다.

policyUsageType(선택 사항), 유형: 문자열

IAM 사용자, IAM 사용자 그룹 또는 역할에 정책을 연결할지 지정합니다. 유효한 값은 IAM_USER, IAM_GROUP, IAM_ROLE 또는 ANY입니다. 기본값은 ANY입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-policy-no-statements-with-admin-access

생성한 AWS Identity and Access Management(IAM) 정책에 모든 리소스의 모든 작업에 권한을 부여하는 Allow 문이 있는지 확인합니다. 고객 관리형 IAM 정책 문에 "Effect": "Allow" with "Action": "*" over "Resource": "*"가 포함된 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 이 규칙은 고객 관리형 정책만 평가합니다. 이 규칙은 인라인 정책 또는 AWS 관리형 정책을 평가하지 않습니다. 차이점에 대한 자세한 내용은 IAM 사용 설명서에서 관리형 정책 및 인라인 정책 페이지를 참조하세요.

다음 정책은 NON_COMPLIANT입니다.

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

다음 정책은 COMPLIANT입니다.

```
"Statement": [
{
"Sid": "VisualEditor",
```

```
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

식별자: IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

리소스 유형: AWS::IAM::Policy

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

excludePermissionBoundaryPolicy(선택 사항), 유형: boolean

> 권한 경계로 사용되는 IAM 정책의 평가를 제외하기 위한 부울 플래그입니다. 'true'로 설정하면 규칙은 평가 시 권한 경계를 포함하지 않습니다. 그렇지 않을 경우 값이 'false'로 설정되면 범위 내의 모든 IAM 정책이 평가됩니다. 기본값은 'false'입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-policy-no-statements-with-full-access

생성한 AWS Identity and Access Management(IAM) 정책이 개별 AWS 리소스의 모든 작업에 권한을 부여하는지 확인합니다. 고객 관리형 IAM 정책이 하나 이상의 AWS 서비스에 대한 전체 액세스를 허용하는 경우 규칙은 NON_COMPLIANT입니다.

컨텍스트: 최소 권한 원칙에 따라 AWS 서비스에 권한을 부여할 때 IAM 정책에서 허용되는 작업을 제한하는 것이 좋습니다. 이 방법은 필요한 작업을 명확하게 지정하여 `ec2:*`와 같은 서비스에 제한 없는 와일드카드를 사용하지 않도록 하여 필요한 권한만 부여하는 데 도움이 됩니다.

경우에 따라 DescribeFlowLogs 및 DescribeAvailabilityZones와 같은 유사한 접두사로 여러 작업에 대한 권한을 허용할 수 있습니다. 이러한 경우에는 접미사가 붙은 와일드카드를 접두사(예: `ec2:Describe*`))에 추가할 수 있습니다. 관련 작업을 그룹화하면 IAM 정책 크기 제한에 도달하지 않도록 하는 데 도움이 될 수 있습니다.

접미사 와일드카드(예: `ec2:Describe*`)와 함께 접두사 작업을 사용하는 경우 이 규칙은 COMPLIANT를 반환합니다. 이 규칙은 무제한 와일드카드(예: `ec2:*`)를 사용하는 경우에만 NON_COMPLIANT를 반환합니다.

> **Note**
>
> 이 규칙은 고객 관리형 정책만 평가합니다. 이 규칙은 인라인 정책 또는 AWS 관리형 정책을 평가하지 않습니다. 차이점에 대한 자세한 내용은 IAM 사용 설명서에서 관리형 정책 및 인라인 정책 페이지를 참조하세요.

식별자: IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

리소스 유형: AWS::IAM::Policy

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

excludePermissionBoundaryPolicy(선택 사항), 유형: boolean

권한 경계로 사용되는 IAM 정책의 평가를 제외하기 위한 부울 플래그입니다. 'true'로 설정하면 규칙은 평가 시 권한 경계를 포함하지 않습니다. 그렇지 않을 경우 값이 'false'로 설정되면 범위 내의 모든 IAM 정책이 평가됩니다. 기본값은 'false'입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-role-managed-policy-check

관리형 정책 목록에 지정된 모든 관리형 정책이 AWS Identity and Access Management(IAM) 역할에 연결되어 있는지 확인합니다. 관리형 정책이 IAM 역할에 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: IAM_ROLE_MANAGED_POLICY_CHECK

리소스 유형: AWS::IAM::Role

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

managedPolicyArns, 유형: CSV

> AWS 관리형 정책 Amazon 리소스 이름(ARNs. 자세한 내용은 IAM 사용 설명서의 Amazon 리소스 이름(ARN) 및 AWS 관리형 정책을 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-root-access-key-check

루트 사용자 액세스 키가 사용 가능한지 확인합니다. 사용자 액세스 키가 없으면 규칙이 COMPLIANT로 간주됩니다. 그렇지 않으면 NON_COMPLIANT로 간주됩니다.

> **Note**
>
> 관리형 규칙 및 글로벌 IAM 리소스 유형
> 2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사용 가능한 AWS 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 리소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에 기록할 수 없습니다. 해당 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.
> 주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.

불필요한 평가를 방지하려면 지원되는 리전 중 하나에만 글로벌 IAM 리소스 유형에 대해 규정 준수를 보고하는 주기적 규칙을 배포해야 합니다. 리전에서 지원되는 관리형 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.

식별자: IAM_ROOT_ACCESS_KEY_CHECK

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-saml-provider-tagged

AWS IAM SAML 공급자에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IAM_SAML_PROVIDER_TAGGED

리소스 유형: AWS::IAM::SAMLProvider

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-server-certificate-expiration-check

AWS IAM에 저장된 IAM SSL/TLS 서버 인증서가 만료되었는지 확인합니다. IAM 서버 인증서가 만료된 경우 규칙은 NON_COMPLIANT입니다.

식별자: IAM_SERVER_CERTIFICATE_EXPIRATION_CHECK

리소스 유형: AWS::IAM::ServerCertificate

트리거 유형: 주기적

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-server-certificate-tagged

AWS IAM 서버 인증서에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IAM_SERVER_CERTIFICATE_TAGGED

리소스 유형: AWS::IAM::ServerCertificate

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-user-group-membership-check

IAM 사용자가 최소 하나의 IAM 그룹에 속하는지 확인합니다.

식별자: IAM_USER_GROUP_MEMBERSHIP_CHECK

리소스 유형: AWS::IAM::User

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

groupNames(선택 사항), 유형: 문자열

IAM 사용자가 속해야 하는 IAM 그룹을 쉼표로 구분한 목록입니다.

> **Note**
>
> 이 규칙은 쉼표가 포함된 그룹 이름을 지원하지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-user-mfa-enabled

AWS Identity and Access Management(IAM) 사용자에게 다중 인증(MFA)이 활성화되어 있는지 확인합니다. 한 명 이상의 IAM 사용자에 대해 MFA가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 관리형 규칙 및 글로벌 IAM 리소스 유형
> 2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사용 가능한 AWS 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 리소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에서는 기록할 수 없습니다. 이러한 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.
> 주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.
> 불필요한 평가를 방지하려면 지원되는 리전 중 하나에만 글로벌 IAM 리소스 유형에 대해 규정 준수를 보고하는 주기적 규칙을 배포해야 합니다. 리전에서 지원되는 관리형 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.

식별자: IAM_USER_MFA_ENABLED

리소스 유형: AWS::IAM::User

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-user-no-policies-check

AWS Identity and Access Management(IAM) 사용자에게 정책이 연결되어 있지 않은지 확인합니다. IAM 사용자는 IAM 그룹 또는 역할에서 받은 권한을 상속해야 합니다. IAM 사용자에 연결된 정책이 최소 한 개 이상 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: IAM_USER_NO_POLICIES_CHECK

리소스 유형: AWS::IAM::User

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iam-user-unused-credentials-check

AWS Identity and Access Management (IAM) 사용자에게 입력한 지정된 일수 내에 사용되지 않은 암호 또는 활성 액세스 키가 있는지 확인합니다. 최근에 사용하지 않은 비활성 계정이 있는 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 재평가 일정

첫 번째 평가 후 4시간 이내에 이 규칙을 재평가하는 것은 결과에 아무런 영향을 주지 않습니다.
관리형 규칙 및 글로벌 IAM 리소스 유형
2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사용 가능한 AWS 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 리소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에서는 기록할 수 없습니다. 해당 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.
주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.
불필요한 평가를 방지하려면 지원되는 리전 중 하나에만 글로벌 IAM 리소스 유형에 대해 규정 준수를 보고하는 주기적 규칙을 배포해야 합니다. 리전에서 지원되는 관리형 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.

식별자: IAM_USER_UNUSED_CREDENTIALS_CHECK

리소스 유형: AWS::IAM::User

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

maxCredentialUsageAge, 유형: int, 기본값: 90

자격 증명을 사용할 수 없는 최대 일수입니다. 기본값은 90일입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

restricted-ssh

> **Important**
>
> 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다.

보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.

식별자: INCOMING_SSH_DISABLED

리소스 유형: AWS::EC2::SecurityGroup

트리거 유형: 구성 변경 및 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

inspector-ec2-scan-enabled

단일 또는 다중 계정 환경에 대해 Amazon Inspector V2 EC2 스캔이 활성화되어 EC2 인스턴스의 잠재적 취약성 및 네트워크 연결성 문제를 감지하는지 확인합니다. EC2 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: INSPECTOR_EC2_SCAN_ENABLED

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

inspector-ecr-scan-enabled

단일 또는 다중 계정 환경에 대해 Amazon Inspector V2 ECR 스캔이 활성화되어 컨테이너 이미지의 잠재적 소프트웨어 취약성을 감지하는지 확인합니다. ECR 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: INSPECTOR_ECR_SCAN_ENABLED

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

inspector-lambda-code-scan-enabled

단일 또는 다중 계정 환경에 대해 Amazon Inspector V2 Lambda 코드 스캔이 활성화되어 잠재적 코드 취약성을 감지하는지 확인합니다. Lambda 코드 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: INSPECTOR_LAMBDA_CODE_SCAN_ENABLED

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 유럽(스톡홀름), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

inspector-lambda-standard-scan-enabled

단일 또는 다중 계정 환경에 대해 Amazon Inspector V2 Lambda 표준 스캔이 활성화되어 잠재적 소프트웨어 취약성을 감지하는지 확인합니다. Lambda 표준 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: INSPECTOR_LAMBDA_STANDARD_SCAN_ENABLED

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ec2-instances-in-vpc

> **Important**
> 이 규칙의 경우 규칙 식별자(INSTANCES_IN_VPC) 와 규칙 이름(ec2-instances-in-vpc)이 서로 다릅니다.

EC2 인스턴스가 Virtual Private Cloud(VPC)에 속하는지 확인합니다. 선택적으로 인스턴스에 할당할 VPC ID를 지정할 수도 있습니다.

식별자: INSTANCES_IN_VPC

리소스 유형: AWS::EC2::Instance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

vpcId(선택 사항), 유형: 문자열

이러한 EC2 인스턴스를 포함하는 VPC의 ID입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

internet-gateway-authorized-vpc-only

인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

식별자: INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

리소스 유형: AWS::EC2::InternetGateway

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

AuthorizedVpcIds(선택 사항), 유형: 문자열

> 연결된 IGW가 있는 권한 있는 VPC ID의 쉼표로 구분된 목록입니다. 매개변수가 제공되지 않으면 연결된 모든 IGW는 NON_COMPLIANT입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iotevents-alarm-model-tagged

AWS IoT Events 경보 모델에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTEVENTS_ALARM_MODEL_TAGGED

리소스 유형: AWS::IoTEvents::AlarmModel

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iotevents-detector-model-tagged

AWS IoT Events 감지기 모델에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTEVENTS_DETECTOR_MODEL_TAGGED

리소스 유형: AWS::IoTEvents::DetectorModel

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iotevents-input-tagged

AWS IoT Events 입력에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTEVENTS_INPUT_TAGGED

리소스 유형: AWS::IoTEvents::Input

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iotsitewise-asset-model-tagged

AWS IoT SiteWise 자산 모델에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTSITEWISE_ASSET_MODEL_TAGGED

리소스 유형: AWS::IoTSiteWise::AssetModel

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iotsitewise-dashboard-tagged

AWS IoT SiteWise 대시보드에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTSITEWISE_DASHBOARD_TAGGED

리소스 유형: AWS::IoTSiteWise::Dashboard

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iotsitewise-gateway-tagged

AWS IoT SiteWise 게이트웨이에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTSITEWISE_GATEWAY_TAGGED

리소스 유형: AWS::IoTSiteWise::Gateway

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iotsitewise-portal-tagged

AWS IoT SiteWise 포털에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTSITEWISE_PORTAL_TAGGED

리소스 유형: AWS::IoTSiteWise::Portal

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iotsitewise-project-tagged

AWS IoT SiteWise 프로젝트에 태그가 있는지 확인합니다. 선택적으로 규칙에 대한 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTSITEWISE_PROJECT_TAGGED

리소스 유형: AWS::IoTSiteWise::Project

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iottwinmaker-component-type-tagged

AWS IoT TwinMaker 구성 요소 유형에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTTWINMAKER_COMPONENT_TYPE_TAGGED

리소스 유형: AWS::IoTTwinMaker::ComponentType

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iottwinmaker-entity-tagged

AWS IoT TwinMaker 엔터티에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTTWINMAKER_ENTITY_TAGGED

리소스 유형: AWS::IoTTwinMaker::Entity

트리거 0유형: 구성 변경

AWS 리전: 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iottwinmaker-scene-tagged

AWS IoT TwinMaker 장면에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTTWINMAKER_SCENE_TAGGED

리소스 유형: AWS::IoTTwinMaker::Scene

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iottwinmaker-sync-job-tagged

AWS IoT TwinMaker 동기화 작업에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTTWINMAKER_SYNC_JOB_TAGGED

리소스 유형: AWS::IoTTwinMaker::SyncJob

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iottwinmaker-workspace-tagged

AWS IoT TwinMaker 워크스페이스에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTTWINMAKER_WORKSPACE_TAGGED

리소스 유형: AWS::IoTTwinMaker::Workspace

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iotwireless-fuota-task-tagged

AWS IoT Wireless FUOTA 작업에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTWIRELESS_FUOTA_TASK_TAGGED

리소스 유형: AWS::IoTWireless::FuotaTask

트리거 0유형: 구성 변경

AWS 리전: 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iotwireless-multicast-group-tagged

AWS IoT Wireless 멀티캐스트 그룹에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTWIRELESS_MULTICAST_GROUP_TAGGED

리소스 유형: AWS::IoTWireless::MulticastGroup

트리거 0유형: 구성 변경

AWS 리전: 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iotwireless-service-profile-tagged

AWS IoT Wireless 서비스 프로파일에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IOTWIRELESS_SERVICE_PROFILE_TAGGED

리소스 유형: AWS::IoTWireless::ServiceProfile

트리거 0유형: 구성 변경

AWS 리전: 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(시드니) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

iot-authorizer-token-signing-enabled

AWS IoT Core 권한 부여자가 권한 부여 요청에서 토큰 서명을 검증하기 위한 서명 요구 사항을 비활성화하지 않았는지 확인합니다. 권한 부여자에 configuration.SigningDisabled가 True로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: IOT_AUTHORIZER_TOKEN_SIGNING_ENABLED

리소스 유형: AWS::IoT::Authorizer

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ivs-channel-playback-authorization-enabled

Amazon IVS 채널에 재생 권한 부여가 활성화되어 있는지 확인합니다. configuration.Authorized가 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: IVS_CHANNEL_PLAYBACK_AUTHORIZATION_ENABLED

리소스 유형: AWS::IVS::Channel

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ivs-channel-tagged

Amazon IVS 채널에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IVS_CHANNEL_TAGGED

리소스 유형: AWS::IVS::Channel

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ivs-playback-key-pair-tagged

Amazon IVS 재생 키 페어에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IVS_PLAYBACK_KEY_PAIR_TAGGED

리소스 유형: AWS::IVS::PlaybackKeyPair

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ivs-recording-configuration-tagged

Amazon IVS 레코딩 구성에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: IVS_RECORDING_CONFIGURATION_TAGGED

리소스 유형: AWS::IVS::RecordingConfiguration

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(도쿄), 미국 서부(오레곤) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

kinesis-firehose-delivery-stream-encrypted

Amazon Kinesis Data Firehose가 서버 측 암호화를 사용하여 저장 시 암호화되는지 확인합니다. Kinesis Data Firehose 전송 스트림이 서버 측 암호화를 사용하여 저장 시 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: KINESIS_FIREHOSE_DELIVERY_STREAM_ENCRYPTED

리소스 유형: AWS::KinesisFirehose::DeliveryStream

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: CSV

Kinesis Firehose 사용이 승인된 KMS 키 ARN을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

kinesis-stream-backup-retention-check

Amazon Kinesis Data Stream의 데이터 기록 보존 기간이 특정 시간 수로 설정되어 있는지 확인합니다. `RetentionPeriodHours` 속성이 파라미터에서 지정된 시간보다 짧은 경우 규칙은 NON_COMPLIANT입니다.

식별자: KINESIS_STREAM_BACKUP_RETENTION_CHECK

리소스 유형: AWS::Kinesis::Stream

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

minimumBackupRetentionPeriod(선택 사항), 유형: 문자열

데이터 레코드를 유지해야 하는 최소 시간입니다. 유효한 값은 24~8760이고 기본값은 168입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

kinesis-stream-encrypted

Amazon Kinesis 스트림이 서버 측 암호화를 사용하여 저장 시 암호화되는지 확인합니다. 'StreamEncryption'이 없는 경우 Kinesis 스트림의 규칙은 NON_COMPLIANT입니다.

컨텍스트: 서버 측 암호화는 AWS KMS 키를 사용하여 저장되기 전에 데이터를 자동으로 암호화하는 Amazon Kinesis Data Streams의 기능입니다. 데이터는 Kinesis 스트림 스토리지 계층에 쓰여지기 전에 암호화되고 스토리지에서 검색된 후 해독됩니다. 결과적으로 데이터는 Kinesis Data Streams 서비스에서 유휴 시 암호화되어 규제 요구 사항을 충족하고 데이터 보안을 강화할 수 있습니다. 자세한 내용은 Amazon Kinesis Data Streams의 데이터 보호를 참조하세요.

식별자: KINESIS_STREAM_ENCRYPTED

리소스 유형: AWS::Kinesis::Stream

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

kms-cmk-not-scheduled-for-deletion

AWS Key Management Service(AWS KMS) 키가 AWS KMS에서 삭제되도록 예약되지 않았는지 확인합니다. KMS 키 삭제가 예약된 경우 규칙은 NON_COMPLIANT입니다.

식별자: KMS_CMK_NOT_SCHEDULED_FOR_DELETION

리소스 유형: AWS::KMS::Key

트리거 유형: 주기적

AWS 리전: 유럽(밀라노), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyIds(선택 사항), 유형: 문자열

(선택 사항) 삭제하도록 예약할 수 없는 특정 고객 관리형 키 ID를 쉼표로 구분한 목록입니다. 키를 지정하지 않으면 이 규칙은 모든 키를 확인합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

kms-key-policy-no-public-access

AWS KMS 키 정책이 퍼블릭 액세스를 허용하는지 확인합니다. KMS 키 정책이 KMS 키에 대한 퍼블릭 액세스를 허용하는 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 비공개로 간주되려면 KMS 키 정책이 고정 값에 대한 액세스 권한만 부여해야 합니다. 즉, 와일드카드 또는 변수라는 IAM 정책 요소가 포함되지 않은 값을 의미합니다https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_variables.html#policy-vars-using-variables.

식별자: KMS_KEY_POLICY_NO_PUBLIC_ACCESS

리소스 유형: AWS::KMS::Key

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

lambda-concurrency-check

Lambda 함수가 함수 수준 동시 실행 한도로 구성되어 있는지 확인합니다. Lambda 함수가 함수 수준 동시 실행 한도로 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: LAMBDA_CONCURRENCY_CHECK

리소스 유형: AWS::Lambda::Function

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

ConcurrencyLimitLow(선택 사항), 유형: 문자열

최소 동시 실행 한도

ConcurrencyLimitHigh(선택 사항), 유형: 문자열

최대 동시 실행 한도

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

lambda-dlq-check

Lambda 함수가 DLQ(Dead Letter Queue)로 구성되어 있는지 확인합니다. Lambda 함수가 DLQ(Dead Letter Queue)로 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: LAMBDA_DLQ_CHECK

리소스 유형: AWS::Lambda::Function

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

dlqArns(선택 사항), 유형: 문자열

Lambda 함수 DLQ(Dead Letter Queue) 대상으로 구성해야 하는 Amazon SQS 및 Amazon SNS ARN을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

lambda-function-public-access-prohibited

Lambda 리소스에 연결된 AWS Lambda 함수 정책이 퍼블릭 액세스를 금지하는지 확인합니다. Lambda 함수 정책이 퍼블릭 액세스를 허용하는 경우 NON_COMPLIANT로 간주됩니다.

컨텍스트: Lambda 함수 정책은 보안 주체 요소가 비어 있거나 와일드카드가 포함된 경우 퍼블릭 액세스를 허용하는 것으로 간주됩니다. 예를 들어, 보안 주체 요소가 “” 또는 `{“AWS”: “”}`인 경우 보안상의 이유로 퍼블릭 액세스 권한을 부여하는 것은 권장되지 않습니다. 퍼블릭 액세스를 제한하면 Lambda 함수의 무단 호출을 방지하는 데 도움이 될 수 있으며, 이로 인해 데이터가 손상되거나 원치 않는 비용이 발생할 수 있습니다.

Lambda 함수에 대한 액세스를 제한하려면 함수를 호출할 수 있는 IAM 사용자, 역할 또는 서비스의 AWS 계정 IDs 또는 Amazon 리소스 이름(ARNs)을 지정합니다. 자세한 정보는 AWS Lambda 개발자 안내서의 다른 계정에 대한 함수 액세스 부여를 참조합니다.

또한 Lambda 함수가 Amazon S3에서 호출되고 정책에와 같은 퍼블릭 액세스를 제한하는 조건이 포함되지 않은 `NON_COMPLIANT` 경우에도 규칙이 적용됩니다`AWS:SourceAccount`. 액세스를 더 세분화하려면 버킷 정책에 `AWS:SourceAccount`와 다른 S3 조건을 함께 사용하는 것이 좋습니다.

> **Note**
>
> 비공개로 간주되려면 Lambda 리소스 기반 정책이 고정 값에 대한 액세스 권한만 부여해야 합니다. 즉, 와일드카드 또는 IAM 정책 요소인 변수가 포함되지 않은 값을 의미합니다.

식별자: LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED

리소스 유형: AWS::Lambda::Function

트리거 0유형: 구성 변경

AWS 리전: 유럽(스페인), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

lambda-function-settings-check

런타임, 역할, 제한 시간 및 메모리 크기에 대한 AWS Lambda 함수 설정이 예상 값과 일치하는지 확인합니다. 규칙은 '이미지' 패키지 유형이 있는 함수와 런타임이 'OS 전용 런타임'으로 설정된 함수를 무시합니다. Lambda 함수 설정이 예상 값과 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: LAMBDA_FUNCTION_SETTINGS_CHECK

리소스 유형: AWS::Lambda::Function

트리거 0유형: 구성 변경

AWS 리전: 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

런타임, 유형: CSV

쉼표로 구분된 AWS Lambda 런타임 값 목록

role(선택 사항), 유형: 문자열

AWS Lambda 실행 역할의 이름 또는 ARN

timeout(선택 사항), 유형: int, 기본값: 3

AWS 초 단위 Lambda 함수 제한 시간

memorySize(선택 사항), 유형: int, 기본값: 128

AWS 메가바이트 단위의 Lambda 함수 크기

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
```

```
...
{
    "MemorySize": Integer*,
    "Role": String*,
    "Runtime": String*,
    "Timeout": Integer*
}
...
```

*이러한 입력의 유효한 값에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 MemorySize, Role, Runtime 및 Timeout을 참조하세요.

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

lambda-function-xray-enabled

AWS Lambda 함수에서 AWS X-Ray가 활성화되어 있는지 확인합니다. Lambda 함수에 대해 X-Ray 추적이 비활성화된 경우 규칙은 NON_COMPLIANT입니다.

식별자: LAMBDA_FUNCTION_XRAY_ENABLED

리소스 유형: AWS::Lambda::Function

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(서울), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

lambda-inside-vpc

Lambda 함수가 Virtual Private Cloud(VPC)에 액세스할 수 있는지 확인합니다. Lambda 함수가 VPC에 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: LAMBDA_INSIDE_VPC

리소스 유형: AWS::Lambda::Function

트리거 0유형: 구성 변경

AWS 리전: 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

subnetIds(선택 사항), 유형: 문자열

Lambda 함수와 연결해야 하는 서브넷 ID를 쉼표로 구분한 목록입니다.

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
   "VpcConfig": {
         "SubnetIds": "[SubnetId-1, SubnetId-2, SubnetId-3, ...]"
   }
}
...
```

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

lambda-vpc-multi-az-check

Lambda에 1개 이상의 가용 영역이 연결되어 있는지 확인합니다. Lambda와 연결된 가용 영역이 1개뿐이거나, 연결된 가용 영역 수가 선택적 파라미터에 지정된 수보다 적은 경우 규칙은 NON_COMPLIANT입니다.

식별자: LAMBDA_VPC_MULTI_AZ_CHECK

리소스 유형: AWS::Lambda::Function

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

availabilityZones(선택 사항), 유형: int

예상 가용 영역의 수입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

lightsail-bucket-tagged

Amazon Lightsail 버킷에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: LIGHTSAIL_BUCKET_TAGGED

리소스 유형: AWS::Lightsail::Bucket

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄),

미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

lightsail-certificate-tagged

Amazon Lightsail 인증서에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: LIGHTSAIL_CERTIFICATE_TAGGED

리소스 유형: AWS::Lightsail::Certificate

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

lightsail-disk-tagged

Amazon Lightsail 디스크에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: LIGHTSAIL_DISK_TAGGED

리소스 유형: AWS::Lightsail::Disk

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

macie-auto-sensitive-data-discovery-check

Amazon Macie에 민감한 데이터 자동 검색이 활성화되어 있는지 확인합니다. 민감한 데이터 자동 검색이 비활성화된 경우 규칙은 NON_COMPLIANT입니다. 이 규칙은 관리자 계정에는 APPLICABLE, 구성원 계정에는 NOT_APPLICABLE입니다.

식별자: MACIE_AUTO_SENSITIVE_DATA_DISCOVERY_CHECK

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

macie-status-check

리전별 계정에서 Amazon Macie가 활성화되어 있는지 확인합니다. 'status' 속성이 'ENABLED'로 설정되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: MACIE_STATUS_CHECK

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mariadb-publish-logs-to-cloudwatch-logs

Amazon MariaDB 데이터베이스 인스턴스가 Amazon CloudWatch Logs에 로그를 게시하도록 구성되어 있는지 확인합니다. 데이터베이스 인스턴스가 CloudWatch Logs에 로그를 게시하도록 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: MARIADB_PUBLISH_LOGS_TO_CLOUDWATCH_LOGS

리소스 유형: AWS::RDS::DBInstance

트리거 유형: 주기적

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

logTypes(선택 사항), 유형: 문자열

> 확인할 규칙에 대한 로그 유형의 쉼표로 구분된 목록입니다. 제공되지 않은 경우 규칙은 기본 로그 유형인 '오류' 및 '감사'를 확인합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mfa-enabled-for-iam-console-access

콘솔 암호를 사용하는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 AWS 다중 인증(MFA)이 활성화되어 있는지 확인합니다. MFA가 활성화되면 규칙이 COMPLIANT로 간주됩니다.

> **Note**
>
> 재평가 일정
> 첫 번째 평가 후 4시간 이내에 이 규칙을 재평가하는 것은 결과에 아무런 영향을 주지 않습니다.
> 관리형 규칙 및 글로벌 IAM 리소스 유형
> 2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사용 가능한 AWS 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 리

소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에서는 기록할 수 없습니다. 해당 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.
주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.
불필요한 평가를 방지하려면 지원되는 리전 중 하나에만 글로벌 IAM 리소스 유형에 대해 규정 준수를 보고하는 주기적 규칙을 배포해야 합니다. 리전에서 지원되는 관리형 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.

식별자: MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

리소스 유형: AWS::IAM::User

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mq-active-broker-ldap-authentication

Amazon MQ ActiveMQ 브로커가 LDAP 인증 전략을 사용하여 브로커를 보호하는지 확인합니다. configuration.AuthenticationStrategy가 'ldap'이 아닌 경우 규칙은 NON_COMPLIANT입니다.

식별자: MQ_ACTIVE_BROKER_LDAP_AUTHENTICATION

리소스 유형: AWS::AmazonMQ::Broker

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mq-active-deployment-mode

Amazon MQ ActiveMQ 브로커 엔진에 대해 구성된 배포 모드를 확인합니다. 기본 단일 인스턴스 브로커 모드를 사용 중인 경우 규칙은 NON_COMPLIANT입니다.

식별자: MQ_ACTIVE_DEPLOYMENT_MODE

리소스 유형: AWS::AmazonMQ::Broker

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mq-active-single-instance-broker-storage-type-efs

mq.m5 인스턴스 유형 패밀리를 사용하는 ActiveMQ용 Amazon MQ 단일 인스턴스 브로커가 브로커 스토리지용 Amazon Elastic File System(EFS)으로 구성되어 있는지 확인합니다. ActiveMQ configuration.StorageType이 'efs'가 아닌 경우 규칙은 NON_COMPLIANT입니다.

식별자: MQ_ACTIVE_SINGLE_INSTANCE_BROKER_STORAGE_TYPE_EFS

리소스 유형: AWS::AmazonMQ::Broker

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mq-automatic-minor-version-upgrade-enabled

마이너 버전 자동 업그레이드가 Amazon MQ 브로커에 대해 활성화되어 있는지 확인합니다. 'AutoMinorVersionUpgrade' 필드가 Amazon MQ 브로커에 대해 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

리소스 유형: AWS::AmazonMQ::Broker

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mq-auto-minor-version-upgrade-enabled

마이너 버전 자동 업그레이드가 Amazon MQ 브로커에 대해 활성화되어 있는지 확인합니다. 'AutoMinorVersionUpgrade' 필드가 Amazon MQ 브로커에 대해 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: MQ_AUTO_MINOR_VERSION_UPGRADE_ENABLED

리소스 유형: AWS::AmazonMQ::Broker

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mq-broker-general-logging-enabled

Amazon MQ 브로커에 일반 로깅이 활성화되어 있는지 확인합니다. configuration.Logs.General이 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: MQ_BROKER_GENERAL_LOGGING_ENABLED

리소스 유형: AWS::AmazonMQ::Broker

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mq-cloudwatch-audit-logging-enabled

Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED

리소스 유형: AWS::AmazonMQ::Broker

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mq-cloudwatch-audit-log-enabled

Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: MQ_CLOUDWATCH_AUDIT_LOG_ENABLED

리소스 유형: AWS::AmazonMQ::Broker

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mq-no-public-access

Amazon MQ 브로커가 퍼블릭 액세스 불가능한지 확인합니다. Amazon MQ 브로커에 대해 'PubliclyAccessible' 필드가 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: MQ_NO_PUBLIC_ACCESS

리소스 유형: AWS::AmazonMQ::Broker

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아프리카(케이프타운), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

mq-rabbit-deployment-mode

Amazon MQ RabbitMQ 브로커 엔진에 대해 구성된 배포 모드를 확인합니다. 기본 단일 인스턴스 브로커 모드를 사용 중인 경우 규칙은 NON_COMPLIANT입니다.

식별자: MQ_RABBIT_DEPLOYMENT_MODE

리소스 유형: AWS::AmazonMQ::Broker

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

msk-cluster-public-access-disabled

Amazon MSK 클러스터에서 퍼블릭 액세스가 비활성화되어 있는지 확인합니다. Amazon MSK 클러스터의 퍼블릭 액세스가 비활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: MSK_CLUSTER_PUBLIC_ACCESS_DISABLED

리소스 유형: AWS::MSK::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(서울), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

msk-connect-connector-logging-enabled

Amazon MSK 커넥터에 로그 대상 중 하나에 대한 로깅이 활성화되어 있는지 확인합니다. Amazon MSK Connector에 로깅이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: MSK_CONNECT_CONNECTOR_LOGGING_ENABLED

리소스 유형: AWS::KafkaConnect::Connector

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

msk-enhanced-monitoring-enabled

PER_TOPIC_PER_BROKER 또는 PER_TOPIC_PER_PARTITION으로 설정된 Amazon MSK 클러스터에 대해 확장 모니터링이 활성화되어 있는지 확인합니다. 확장 모니터링이 활성화되어 있고, DEFAULT 또는 PER_BROKER로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: MSK_ENHANCED_MONITORING_ENABLED

리소스 유형: AWS::MSK::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

msk-in-cluster-node-require-tls

Amazon MSK 클러스터가 클러스터의 브로커 노드와 함께 HTTPS(TLS)를 사용하여 전송 중 암호화를 적용하는지 확인합니다. 클러스터 내 브로커 노드 연결에 대해 일반 텍스트 통신이 활성화된 경우 규칙은 NON_COMPLIANT입니다.

식별자: MSK_IN_CLUSTER_NODE_REQUIRE_TLS

리소스 유형: AWS::MSK::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

msk-unrestricted-access-check

Amazon MSK 클러스터에 인증되지 않은 액세스가 비활성화되어 있는지 확인합니다. Amazon MSK 클러스터에 인증되지 않은 액세스가 활성화된 경우 규칙은 NON_COMPLIANT입니다.

식별자: MSK_UNRESTRICTED_ACCESS_CHECK

리소스 유형: AWS::MSK::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(서울), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

multi-region-cloudtrail-enabled

> **Important**
>
> 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다.

다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. `ExcludeManagementEventSources` 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

식별자: MULTI_REGION_CLOUD_TRAIL_ENABLED

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

s3BucketName(선택 사항), 유형: 문자열

로그 파일을 전송할 AWS CloudTrail용 Amazon S3 버킷의 이름입니다.

snsTopicArn(선택 사항), 유형: 문자열

알림에 사용할 Amazon SNS 주제 ARN for AWS CloudTrail입니다.

cloudWatchLogsLogGroupArn(선택 사항), 유형: 문자열

데이터를 전송할 AWS CloudTrail용 Amazon CloudWatch 로그 그룹 ARN입니다.

includeManagementEvents(선택 사항), 유형: boolean

AWS CloudTrail에 대한 관리 이벤트를 포함하는 이벤트 선택기입니다.

readWriteType(선택 사항), 유형: 문자열

기록할 이벤트의 유형입니다. 유효한 값은 ReadOnly, WriteOnly, ALL입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

nacl-no-unrestricted-ssh-rdp

네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한이 없는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.

식별자: NACL_NO_UNRESTRICTED_SSH_RDP

리소스 유형: AWS::EC2::NetworkAcl

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

neptune-cluster-backup-retention-check

Amazon Neptune DB 클러스터 보존 기간이 특정 일수로 설정되어 있는지 확인합니다. 보존 기간이 파라미터에서 지정된 값보다 짧은 경우 규칙은 NON_COMPLIANT입니다.

식별자: NEPTUNE_CLUSTER_BACKUP_RETENTION_CHECK

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

minimumBackupRetentionPeriod(선택 사항), 유형: int

> 백업을 보관해야 할 최소 기간(일)입니다. 유효한 값은 1~35이며, 기본값은 7입니다. 값이 'backupRetentionPeriod'보다 큰 경우 규칙은 NON_COMPLIANT입니다. 값이 'backupRetentionPeriod'보다 작거나 같을 경우 규칙은 COMPLIANT입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

neptune-cluster-cloudwatch-log-export-enabled

Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: NEPTUNE_CLUSTER_CLOUDWATCH_LOG_EXPORT_ENABLED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

neptune-cluster-copy-tags-to-snapshot-enabled

스냅샷이 생성될 때 Amazon Neptune 클러스터가 모든 태그를 스냅샷에 복사하도록 구성되어 있는지 확인합니다. 'copyTagsToSnapshot'이 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: NEPTUNE_CLUSTER_COPY_TAGS_TO_SNAPSHOT_ENABLED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

neptune-cluster-deletion-protection-enabled

Amazon Neptune DB 클러스터에 삭제 방지가 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터의 삭제 방지 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: NEPTUNE_CLUSTER_DELETION_PROTECTION_ENABLED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

neptune-cluster-encrypted

Amazon Neptune DB 클러스터에 스토리지 암호화가 활성화되어 있는지 확인합니다. 스토리지 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: NEPTUNE_CLUSTER_ENCRYPTED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

KmsKeyArns(선택 사항), 유형: CSV

암호화된 클러스터의 KmsKeyId와 비교할 수 있는 KMS 키 ARN을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

neptune-cluster-iam-database-authentication

Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: NEPTUNE_CLUSTER_IAM_DATABASE_AUTHENTICATION

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

neptune-cluster-multi-az-enabled

Amazon Neptune 클러스터에 Amazon RDS 다중 AZ 복제가 구성되어 있는지 확인합니다. 다중 AZ 복제가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: NEPTUNE_CLUSTER_MULTI_AZ_ENABLED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

neptune-cluster-snapshot-encrypted

Amazon Neptune DB 클러스터에 암호화된 스냅샷이 있는지 확인합니다. Neptune 클러스터에 암호화된 스냅샷이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: NEPTUNE_CLUSTER_SNAPSHOT_ENCRYPTED

리소스 유형: AWS::RDS::DBClusterSnapshot

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

neptune-cluster-snapshot-public-prohibited

Amazon Neptune 수동 DB 클러스터 스냅샷이 퍼블릭인지 확인합니다. 기존 및 신규 Neptune 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

식별자: NEPTUNE_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

리소스 유형: AWS::RDS::DBClusterSnapshot

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

netfw-deletion-protection-enabled

AWS Network Firewall에 삭제 방지 기능이 활성화되어 있는지 확인합니다. Network Firewall에 삭제 방지 기능이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: NETFW_DELETION_PROTECTION_ENABLED

리소스 유형: AWS::NetworkFirewall::Firewall

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

netfw-logging-enabled

AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.

식별자: NETFW_LOGGING_ENABLED

리소스 유형: AWS::NetworkFirewall::LoggingConfiguration

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

logType(선택 사항), 유형: 문자열

logType(선택 사항): 방화벽을 확인하기 위한 규칙의 로그 유형인 'alert', 'flow' 또는 'both'입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

netfw-multi-az-enabled

AWS Network Firewall 방화벽이 여러 가용 영역에 배포되었는지 확인합니다. 방화벽이 하나의 가용 영역에만 배포되거나, 선택적 파라미터에 나열된 수보다 적은 수의 영역에 배포된 경우 규칙은 NON_COMPLIANT입니다.

식별자: NETFW_MULTI_AZ_ENABLED

리소스 유형: AWS::NetworkFirewall::Firewall

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

availabilityZones(선택 사항), 유형: int

예상 가용 영역의 수입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

netfw-policy-default-action-fragment-packets

AWS Network Firewall 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

식별자: NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS

리소스 유형: AWS::NetworkFirewall::FirewallPolicy

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

statelessFragmentDefaultActions, 유형: CSV

쉼표로 구분된 값 목록입니다. 최대 두 개를 선택할 수 있습니다. 유효한 값으로는 'aws:pass', 'aws:drop', 'aws:forward_to_sfe'가 포함됩니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

netfw-policy-default-action-full-packets

AWS Network Firewall 정책이 전체 패킷에 대해 사용자 정의 기본 상태 비저장 작업으로 구성되어 있는지 확인합니다. 전체 기본 상태 비저장 작업이 사용자 정의 기본 상태 비저장 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

식별자: NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS

리소스 유형: AWS::NetworkFirewall::FirewallPolicy

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

statelessDefaultActions, 유형: CSV

> 쉼표로 구분된 값 목록입니다. 최대 두 개를 선택할 수 있습니다. 유효한 값으로는 'aws:pass', 'aws:drop', 'aws:forward_to_sfe'가 포함됩니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

netfw-policy-rule-group-associated

AWS Network Firewall 정책이 상태 저장 또는 상태 비저장 규칙 그룹과 연결되어 있는지 확인합니다. 상태 저장 또는 상태 비저장 규칙 그룹이 Network Firewall 정책에 연결되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 또는 규칙 그룹 중 하나가 존재할 경우 이 규칙은 COMPLIANT입니다.

식별자: NETFW_POLICY_RULE_GROUP_ASSOCIATED

리소스 유형: AWS::NetworkFirewall::FirewallPolicy

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

netfw-stateless-rule-group-not-empty

Stateless Network Firewall 규칙 그룹에 규칙이 포함되어 있는지 확인합니다. Stateless Network Firewall 규칙 그룹에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

리소스 유형: AWS::NetworkFirewall::RuleGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

netfw-subnet-change-protection-enabled

AWS Network Firewall에 서브넷 변경 보호가 활성화되어 있는지 확인합니다. 서브넷 변경 방지가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: NETFW_SUBNET_CHANGE_PROTECTION_ENABLED

리소스 유형: AWS::NetworkFirewall::Firewall

트리거 0유형: 구성 변경

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

nlb-cross-zone-load-balancing-enabled

Network Load Balancer(NLB)에 대해 교차 영역 로드 밸런싱이 활성화되어 있는지 확인합니다. NLB에 대해 교차 영역 로드 밸런싱이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

리소스 유형: AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

nlb-internal-scheme-check

Network Load Balancer 체계가 내부인지 확인합니다. configuration.scheme이 내부로 설정되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: NLB_INTERNAL_SCHEME_CHECK

리소스 유형: AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

nlb-listener-tagged

Network Load Balancer 리스너에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: NLB_LISTENER_TAGGED

리소스 유형: AWS::ElasticLoadBalancingV2::Listener

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

nlb-logging-enabled

Network Load Balancer에 액세스 로깅이 활성화되어 있는지 확인합니다. Network Load Balancer에 대한 액세스 로깅이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: NLB_LOGGING_ENABLED

리소스 유형: AWS::ElasticLoadBalancingV2::LoadBalancer

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

no-unrestricted-route-to-igw

라우팅 테이블에 인터넷 게이트웨이(IGW)로 연결되는 퍼블릭 경로가 있는지 확인합니다. IGW에 대한 경로의 대상 CIDR 블록이 '0.0.0.0/0' 또는 '::/0'이거나, 대상 CIDR 블록이 규칙 파라미터와 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: NO_UNRESTRICTED_ROUTE_TO_IGW

리소스 유형: AWS::EC2::RouteTable

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

routeTableIds(선택 사항), 유형: CSV

대상 CIDR 블록이 '0.0.0.0/0' 또는 '::/0'인 인터넷 게이트웨이에 대한 경로를 가질 수 있는 라우팅 테이블 ID를 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

opensearch-access-control-enabled

Amazon OpenSearch Service 도메인에 세분화된 액세스 제어가 활성화되어 있는지 확인합니다. OpenSearch Service 도메인에 대해 AdvancedSecurityOptions가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: OPENSEARCH_ACCESS_CONTROL_ENABLED

리소스 유형: AWS::OpenSearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

opensearch-audit-logging-enabled

Amazon OpenSearch Service 도메인에 감사 로깅이 활성화되어 있는지 확인합니다. OpenSearch Service 도메인에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: OPENSEARCH_AUDIT_LOGGING_ENABLED

리소스 유형: AWS::OpenSearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

cloudWatchLogsLogGroupArnList(선택 사항), 유형: CSV

> Amazon CloudWatch Logs 로그 그룹에 대한 Amazon 리소스 이름(ARN)을 쉼표로 구분한 목록입니다. 규칙이 감사 로그에 대해 지정된 로그 그룹이 구성되어 있는지 확인합니다.
>
> 유효값은 `arn:aws:logs:region:account-id:log-group:log_group_name:*`, `arn:aws:logs:region:account-id:log-group:log_group_name`입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

opensearch-data-node-fault-tolerance

Amazon OpenSearch Service 도메인이 최소 세 개의 데이터 노드로 구성되어 있고 zoneAwarenessEnabled기 true인지 확인합니다. 'instanceCount'가 3개 미만이거나 'zoneAwarenessEnabled'가 'false'로 설정된 경우 OpenSearch 도메인에 대한 규칙은 NON_COMPLIANT입니다.

식별자: OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

리소스 유형: AWS::OpenSearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

opensearch-encrypted-at-rest

Amazon OpenSearch Service 도메인에 저장 시 암호화 구성이 활성화되어 있는지 확인합니다. `EncryptionAtRestOptions` 필드가 활성화되어 있지 않으면 규칙은 NON_COMPLIANT입니다.

> **Note**
> 규칙은 Elasticsearch 도메인을 평가하지 않습니다.

식별자: OPENSEARCH_ENCRYPTED_AT_REST

리소스 유형: AWS::OpenSearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

opensearch-https-required

OpenSearch 도메인에 대한 연결이 HTTPS를 사용하고 있는지 확인합니다. Amazon OpenSearch 도메인 'EnforceHTTPS'가 'true'가 아닌 경우 또는 'true'이지만 'TLSSecurityPolicy'가 '`tlsPolicies`'에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: OPENSEARCH_HTTPS_REQUIRED

리소스 유형: AWS::OpenSearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

tlsPolicies(선택 사항), 유형: CSV

Amazon OpenSearch 도메인과 비교하여 확인할 TLS 보안 정책을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

opensearch-in-vpc-only

Amazon OpenSearch Service 도메인이 Amazon Virtual Private Cloud(VPC)에 있는지 확인합니다. OpenSearch Service 도메인 엔드포인트가 퍼블릭이면 규칙은 NON_COMPLIANT입니다.

> **Note**
> 규칙은 Elasticsearch 도메인을 평가하지 않습니다.

식별자: OPENSEARCH_IN_VPC_ONLY

리소스 유형: AWS::OpenSearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

opensearch-logs-to-cloudwatch

Amazon CloudWatch Logs에 로그를 전송하도록 Amazon OpenSearch Service 도메인이 구성되어 있는지 확인합니다. 로깅이 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
> 규칙은 Elasticsearch 도메인을 평가하지 않습니다.

식별자: OPENSEARCH_LOGS_TO_CLOUDWATCH

리소스 유형: AWS::OpenSearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

logTypes(선택 사항), 유형: CSV

활성화된 로그를 쉼표로 구분한 목록입니다. 유효한 값은 'search', 'index', 'error'입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

opensearch-node-to-node-encryption-check

Amazon OpenSearch Service 노드가 처음부터 끝까지 암호화되어 있는지 확인합니다. 도메인에서 노드 간 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
> 규칙은 Elasticsearch 도메인을 평가하지 않습니다.

식별자: OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

리소스 유형: AWS::OpenSearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

opensearch-primary-node-fault-tolerance

Amazon OpenSearch Service 도메인이 3개 이상의 전용 프라이머리 노드로 구성되어 있는지 확인합니다. 'DedicatedMasterEnabled'가 'false'로 설정되거나 'DedicatedMasterCount'가 3 미만인 경우 OpenSearch Service 도메인의 규칙은 NON_COMPLIANT입니다.

식별자: OPENSEARCH_PRIMARY_NODE_FAULT_TOLERANCE

리소스 유형: AWS::OpenSearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

opensearch-update-check

Amazon OpenSearch Service 버전 업데이트를 사용할 수 있지만 설치되지 않았는지 확인합니다. 최신 소프트웨어 업데이트가 설치되지 않은 경우 OpenSearch 도메인에 대한 규칙은 NON_COMPLIANT입니다.

식별자: OPENSEARCH_UPDATE_CHECK

리소스 유형: AWS::OpenSearch::Domain

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rabbit-mq-supported-version

Amazon MQ RabbitMQ 브로커가 지정된 최소 지원 엔진 버전에서 실행 중인지 확인합니다. RabbitMQ 브로커가 지정한 지원되는 최소 엔진 버전에서 실행되지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: RABBIT_MQ_SUPPORTED_VERSION

리소스 유형: AWS::AmazonMQ::Broker

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

supportedEngineVersion, 유형: 문자열

> RabbitMQ 브로커를 지원하는 최소 엔진 버전을 확인하는 규칙의 문자열 값입니다. RabbitMQ 브로커는 의미 체계 버전 지정 사양(X.Y.Z)을 사용합니다. X는 메이저 버전, Y는 마이너 버전, Z는 패치 버전을 의미합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-aurora-mysql-audit-logging-enabled

Amazon Aurora MySQL 호환 에디션 클러스터가 Amazon CloudWatch Logs에 감사 로그를 게시하도록 구성되었는지 확인합니다. Aurora MySQL 호환 에디션 클러스터에 감사 로그 게시가 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_AURORA_MYSQL_AUDIT_LOGGING_ENABLED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-aurora-postgresql-logs-to-cloudwatch

Amazon Aurora PostgreSQL DB 클러스터가 PostgreSQL 로그를 Amazon CloudWatch Logs에 게시하도록 구성되어 있는지 확인합니다. DB 클러스터가 PostgreSQL 로그를 Amazon CloudWatch Logs에 게시하도록 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: RDS_AURORA_POSTGRESQL_LOGS_TO_CLOUDWATCH

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-automatic-minor-version-upgrade-enabled

Amazon Relational Database Service(RDS) 데이터베이스 인스턴스에 자동 마이너 버전 업그레이드가 구성되어 있는지 확인합니다. 'autoMinorVersionUpgrade' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
...
```

*이러한 입력의 유효한 값에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 AutoMinorVersionUpgrade 및 Engine을 참조하세요.

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-cluster-auto-minor-version-upgrade-enable

Amazon RDS 다중 AZ 클러스터 배포에 자동 마이너 버전 업그레이드가 활성화되어 있는지 확인합니다. autoMinorVersionUpgrade가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_CLUSTER_AUTO_MINOR_VERSION_UPGRADE_ENABLE

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 미국 서부(캘리포니아 북부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-cluster-default-admin-check

Amazon Relational Database Service(RDS) 데이터베이스 클러스터가 관리자 사용자 이름을 기본값에서 변경했는지 확인합니다. 관리자 사용자 이름이 기본값으로 설정되어 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_CLUSTER_DEFAULT_ADMIN_CHECK

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

validAdminUserNames(선택 사항), 유형: CSV

> Amazon RDS 클러스터가 사용할 수 있는 관리자 사용자 이름을 쉼표로 구분한 목록입니다. 'postgres' 또는 'admin'은 기본값이므로 유효한 사용자 이름으로 포함할 수 없습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-cluster-deletion-protection-enabled

Amazon Relational Database Service(RDS) 클러스터에 삭제 방지 기능이 활성화되어 있는지 확인합니다. Amazon RDS 클러스터에 삭제 방지 기능이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_CLUSTER_DELETION_PROTECTION_ENABLED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-cluster-encrypted-at-rest

Amazon Relational Database Service(RDS) 클러스터가 저장 시 암호화되는지 확인합니다. Amazon RDS 클러스터가 저장 시 암호화되지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_CLUSTER_ENCRYPTED_AT_REST

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-cluster-iam-authentication-enabled

Amazon Relational Database Service(RDS) 클러스터에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 클러스터에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-cluster-multi-az-enabled

Amazon Relational Database Service(RDS)에서 관리하는 Amazon Aurora 및 다중 AZ DB 클러스터에서 다중 가용 영역(다중 AZ) 복제가 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스가 다중 AZ로 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_CLUSTER_MULTI_AZ_ENABLED

리소스 유형: AWS::RDS::DBCluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(멜버른) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-db-security-group-not-allowed

기본 DB 보안 그룹이 아닌 Amazon Relational Database Service(RDS) DB 보안 그룹이 있는지 확인합니다. 기본 DB 보안 그룹이 아닌 DB 보안 그룹이 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_DB_SECURITY_GROUP_NOT_ALLOWED

리소스 유형: AWS::RDS::DBSecurityGroup

트리거 0유형: 구성 변경

AWS 리전: 유럽(아일랜드), 남아메리카(상파울루), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니) 리전에서만 사용 가능합니다.

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-enhanced-monitoring-enabled

Amazon RDS 인스턴스에 향상된 모니터링이 활성화되어 있는지 확인합니다. RDS 인스턴스의 구성 항목에서 'monitoringInterval'이 '0'이거나, 'monitoringInterval'이 규칙 파라미터 값과 일치하지 않는 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: RDS_ENHANCED_MONITORING_ENABLED

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

monitoringInterval(선택 사항), 유형: int

> 데이터베이스 인스턴스에 대한 확장 모니터링 지표를 수집하는 시점 사이의 정수 값 간격(초)입니다. 유효한 값은 1, 5, 10, 15, 30, 60입니다.

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

*이러한 입력의 유효한 값에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 MonitoringInterval 및 Engine을 참조하세요.

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-instance-default-admin-check

Amazon Relational Database Service(RDS) 데이터베이스가 관리자 사용자 이름을 기본값에서 변경했는지 확인합니다. 이 규칙은 RDS 데이터베이스 인스턴스에서만 실행됩니다. 관리자 사용자 이름이 기본값으로 설정되어 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_INSTANCE_DEFAULT_ADMIN_CHECK

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

validAdminUserNames(선택 사항), 유형: CSV

> Amazon RDS 인스턴스가 사용할 수 있는 관리자 사용자 이름을 쉼표로 구분한 목록입니다. ('postgres' 또는 'admin'은 기본값이므로 유효한 사용자 이름으로 포함할 수 없습니다.)

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-instance-deletion-protection-enabled

Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스에 삭제 방지 기능이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다. 예를 들어, deletionProtection이 false로 설정되어 있습니다.

> **Warning**
> 클러스터 내의 일부 RDS DB 인스턴스(Aurora/DocumentDB)는 규정 미준수로 표시됩니다.

식별자: RDS_INSTANCE_DELETION_PROTECTION_ENABLED

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

databaseEngines(선택 사항), 유형: CSV

> 규칙 평가에 포함할 RDS 데이터베이스 엔진을 쉼표로 구분한 목록입니다. 'mysql, postgres, mariadb'를 예로 들 수 있습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-instance-iam-authentication-enabled

Amazon Relational Database Service(RDS) 인스턴스에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
> DB 엔진은 'mysql', 'postgres', 'aurora', 'aurora-mysql' 또는 'aurora-postgresql' 중 하나여야 합니다. DB 인스턴스 상태는 'available', 'backing-up', 'storage-optimization' 또는 'storage-full' 중 하나여야 합니다.

식별자: RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-instance-public-access-check

Amazon Relational Database Service(RDS) 인스턴스가 퍼블릭 액세스 불가능한지 확인합니다. 인스턴스 구성 항목에서 publiclyAccessible 필드가 true인 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_INSTANCE_PUBLIC_ACCESS_CHECK

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
```

```
{
   "PubliclyAccessible": BOOLEAN
}
...
```

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-instance-subnet-igw-check

인터넷 게이트웨이 경로가 있는 퍼블릭 서브넷에 RDS DB 인스턴스가 배포되었는지 확인합니다. RDS DB 인스턴스가 퍼블릭 서브넷에 배포된 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_INSTANCE_SUBNET_IGW_CHECK

리소스 유형: AWS::RDS::DBInstance

트리거 유형: 주기적

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-in-backup-plan

Amazon Relational Database Service(RDS) 데이터베이스가 AWS 백업 계획에 있는지 확인합니다. Amazon RDS 데이터베이스가 AWS 백업 계획에 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
> 이 규칙은 Amazon Aurora DB 인스턴스에만 적용됩니다. DB 클러스터는 지원되지 않습니다.

식별자: RDS_IN_BACKUP_PLAN

리소스 유형: AWS::RDS::DBInstance

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-last-backup-recovery-point-created

Amazon Relational Database Service(RDS)에 대한 복구 시점이 생성되었는지 확인합니다. 지정된 기간 내에 생성된 해당하는 복구 시점이 Amazon RDS 인스턴스에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_LAST_BACKUP_RECOVERY_POINT_CREATED

리소스 유형: AWS::RDS::DBInstance

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon RDS 인스턴스의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon RDS 인스턴스의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 744시간, 일수는 31일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-logging-enabled

Amazon Relational Database Service(RDS)의 각 로그가 활성화되어 있는지 확인합니다. 로그 유형이 활성화되어 있지 않으면 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 'available', 'backing-up', 'storage-optimization' 또는 'storage-full' 상태가 아닌 DB 인스턴스는 `NOT_APPLICABLE`로 평가됩니다.

식별자: RDS_LOGGING_ENABLED

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

additionalLogs(선택 사항), 유형: StringMap

엔진 이름과 로그 유형 이름을 쉼표로 구분한 목록입니다. 예를 들어 "additionalLogs": "oracle: general, slowquery ; aurora: alert, slowquery"가 이에 해당합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-mariadb-instance-encrypted-in-transit

엔진 버전이 10.5 이상인 Amazon RDS for MariaDB DB 인스턴스에 대한 연결이 전송 중 암호화를 사용하는지 확인합니다. DB 파라미터 그룹이 동기화되지 않거나 require_secure_transport가 ON으로 설정되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_MARIADB_INSTANCE_ENCRYPTED_IN_TRANSIT

리소스 유형: AWS::RDS::DBInstance

트리거 유형: 주기적

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-meets-restore-time-target

Amazon Relational Database Service(RDS) 인스턴스의 복원 시간이 지정된 기간을 충족하는지 확인합니다. Amazon RDS 인스턴스의 LatestRestoreExecutionTimeMinutes가 maxRestoreTime(분)보다 큰 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_MEETS_RESTORE_TIME_TARGET

리소스 유형: AWS::RDS::DBInstance

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

maxRestoreTime, 유형: int

허용되는 최대 복원 런타임의 숫자 값입니다.

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon RDS 인스턴스의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon RDS 인스턴스의 ID입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-multi-az-support

RDS DB 인스턴스에 고가용성이 활성화되어 있는지 확인합니다.

다중 AZ 배포에서 Amazon RDS는 자동으로 서로 다른 가용 영역에 동기식 예비 복제본을 프로비저닝하고 유지합니다. 자세한 내용을 알아보려면 Amazon RDS 사용 설명서의 고가용성(다중 AZ)를 참조하세요.

> **Note**
>
> 이 규칙은 Amazon Aurora DB, Amazon DocumentDB, Amazon Neptune DB 인스턴스를 평가하지 않습니다.

식별자: RDS_MULTI_AZ_SUPPORT

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

*이러한 입력의 유효한 값에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 MultiAZ and Engine을 참조하세요.

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-mysql-instance-encrypted-in-transit

Amazon RDS for MySQL 데이터베이스 인스턴스에 대한 연결이 전송 중 암호화를 사용하도록 구성되어 있는지 확인합니다. 연결된 데이터베이스 파라미터 그룹이 동기화되지 않거나 require_secure_transport 파라미터가 1로 설정되지 않은 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> Amazon RDS 인스턴스가 RDS 클러스터의 일부인 `NOT_APPLICABLE` 경우 규칙이를 반환합니다.

식별자: RDS_MYSQL_INSTANCE_ENCRYPTED_IN_TRANSIT

리소스 유형: AWS::RDS::DBInstance

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-postgresql-logs-to-cloudwatch

Amazon PostgreSQL DB 인스턴스가 Amazon CloudWatch Logs에 로그를 게시하도록 구성되어 있는지 확인합니다. DB 인스턴스가 Amazon CloudWatch Logs에 로그를 게시하도록 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_POSTGRESQL_LOGS_TO_CLOUDWATCH

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

logTypes(선택 사항), 유형: CSV

> CloudWatch Logs에 게시할 로그 유형의 쉼표로 구분된 목록 유효한 값은 'postgresql', 'upgrade'입니다. 기본값은 'postgresql'입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-postgres-instance-encrypted-in-transit

Amazon RDS PostgreSQL 데이터베이스 인스턴스에 대한 연결이 전송 중 암호화를 사용하도록 구성되어 있는지 확인합니다. 연결된 데이터베이스 파라미터 그룹이 동기화되지 않거나 rds.force_ssl 파라미터가 1로 설정되지 않은 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> Amazon RDS 인스턴스가 RDS 클러스터의 일부인 `NOT_APPLICABLE` 경우 규칙이를 반환합니다.

식별자: RDS_POSTGRES_INSTANCE_ENCRYPTED_IN_TRANSIT

리소스 유형: AWS::RDS::DBInstance

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-proxy-tls-encryption

Amazon RDS 프록시가 모든 연결에 TLS를 적용하는지 확인합니다. Amazon RDS 프록시에 모든 연결에 TLS가 적용되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_PROXY_TLS_ENCRYPTION

리소스 유형: AWS::RDS::DBProxy

트리거 유형: 주기적

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-resources-protected-by-backup-plan

Amazon Relational Database Service(RDS) 인스턴스가 백업 계획에 의해 보호되는지 확인합니다. Amazon RDS 인스턴스를 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

리소스 유형: AWS::RDS::DBInstance

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon RDS 인스턴스의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon RDS 인스턴스의 ID입니다.

crossRegionList(선택 사항), 유형: 문자열

리전 간 백업 사본을 보관할 대상 리전을 쉼표로 구분한 목록입니다.

crossAccountList(선택 사항), 유형: 문자열

계정 간 백업 사본을 보관할 대상 계정을 쉼표로 구분한 목록입니다.

maxRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최대 보존 기간(일)

minRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최소 보존 기간(일)

backupVaultLockCheck(선택 사항), 유형: 문자열

허용되는 값: 'True' 또는 'False'. 리소스가 잠긴 볼트에 백업되어 있는지 확인하는 규칙에 'True'를 입력합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-snapshots-public-prohibited

Amazon Relational Database Service(RDS) 스냅샷이 퍼블릭인지 확인합니다. 기존 및 신규 Amazon RDS 스냅샷이 퍼블릭인 경우 규칙이 NON_COMPLIANT로 간주됩니다.

> **Note**
> 규정 준수 결과를 캡처하는 데 최대 12시간이 걸릴 수 있습니다.

식별자: RDS_SNAPSHOTS_PUBLIC_PROHIBITED

리소스 유형: AWS::RDS::DBSnapshot, AWS::RDS::DBClusterSnapshot

트리거 0유형: 구성 변경

AWS 리전: 아프리카(케이프타운), 아시아 태평양(멜버른), 유럽(밀라노), 이스라엘(텔아비브), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-snapshot-encrypted

Amazon Relational Database Service(RDS) DB 스냅샷이 암호화되는지 확인합니다. Amazon RDS DB 스냅샷이 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_SNAPSHOT_ENCRYPTED

리소스 유형: AWS::RDS::DBSnapshot, AWS::RDS::DBClusterSnapshot

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-sqlserver-encrypted-in-transit

Amazon RDS SQL Server 데이터베이스 인스턴스에 대한 연결이 전송 중 암호화를 사용하도록 구성되어 있는지 확인합니다. 파라미터 그룹의 DB 파라미터 force_ssl이 1로 설정되지 않았거나 ApplyStatus 파라미터가 'in-sync'가 아닌 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_SQLSERVER_ENCRYPTED_IN_TRANSIT

리소스 유형: AWS::RDS::DBInstance

트리거 유형: 주기적

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-sql-server-logs-to-cloudwatch

Amazon SQL Server DB 인스턴스가 Amazon CloudWatch Logs에 로그를 게시하도록 구성되어 있는지 확인합니다. DB 인스턴스가 Amazon CloudWatch Logs에 로그를 게시하도록 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: RDS_SQL_SERVER_LOGS_TO_CLOUDWATCH

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

logTypes(선택 사항), 유형: CSV

> logTypes - (선택 사항): CloudWatch Logs에 게시할 로그 유형의 쉼표로 구분된 목록 유효한 값은 'error', 'agent'입니다. 기본값은 'error', 'agent'입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

rds-storage-encrypted

Amazon Relational Database Service(RDS) DB 인스턴스에 대해 스토리지 암호화가 활성화되어 있는지 확인합니다. 스토리지 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: RDS_STORAGE_ENCRYPTED

리소스 유형: AWS::RDS::DBInstance

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

kmsKeyId(선택 사항), 유형: 문자열

스토리지를 암호화하는 데 사용되는 KMS 키 ID 또는 Amazon 리소스 이름(ARN)입니다.

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
...
```

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-audit-logging-enabled

Amazon Redshift 클러스터가 특정 버킷에 감사를 로깅하는지 확인합니다. Redshift 클러스터에 대해 감사 로깅이 활성화되지 않았거나, 'bucketNames' 파라미터가 제공되었지만 감사 로깅 대상이 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_AUDIT_LOGGING_ENABLED

리소스 유형: AWS::Redshift::Cluster

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

bucketNames(선택 사항), 유형: CSV

감사 로그를 저장하기 위한 Amazon S3 버킷 이름을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-backup-enabled

클러스터에 대해 Amazon Redshift 자동 스냅샷이 활성화되어 있는지 확인합니다. `automatedSnapshotRetentionPeriod`의 값이 `MaxRetentionPeriod`보다 크거나 `MinRetentionPeriod`보다 작거나, 값이 `0`이면 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_BACKUP_ENABLED

리소스 유형: AWS::Redshift::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

MinRetentionPeriod(선택 사항), 유형: int

보존 기간의 최소값입니다. 최소값은 1입니다.

MaxRetentionPeriod(선택 사항), 유형: int

보존 기간의 최소값입니다. 최대값은 35입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-cluster-configuration-check

Amazon Redshift 클러스터에 지정된 설정이 있는지 확인합니다. Amazon Redshift 클러스터가 암호화되지 않았거나 다른 키로 암호화된 경우, 또는 클러스터에 감사 로깅이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_CLUSTER_CONFIGURATION_CHECK

리소스 유형: AWS::Redshift::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 멕시코(중부), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 유럽(스페인) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

clusterDbEncrypted, 유형: boolean, 기본값: true

데이터베이스 암호화가 활성화되어 있습니다.

loggingEnabled, 유형: boolean, 기본값: true

감사 로깅이 활성화되어 있습니다.

nodeTypes(선택 사항), 유형: CSV, 기본값: dc1.large

노드 유형을 지정합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-cluster-kms-enabled

Amazon Redshift 클러스터가 암호화에 지정된 AWS Key Management Service (AWS KMS) 키를 사용하고 있는지 확인합니다. 암호화가 활성화되어 있고 `kmsKeyArn` 파라미터에 제공된 키로 클러스터가 암호화된 경우 규칙은 COMPLIANT입니다. 클러스터가 암호화되지 않거나 다른 키로 암호화된 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_CLUSTER_KMS_ENABLED

리소스 유형: AWS::Redshift::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: CSV

> 암호화를 위해 Amazon Redshift 클러스터에 사용되는 AWS KMS 주요 Amazon 리소스 이름(ARNs)의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-cluster-maintenancesettings-check

Amazon Redshift 클러스터에 지정된 유지 관리 설정이 있는지 확인합니다. 메이저 버전으로의 자동 업그레이드가 비활성화된 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

리소스 유형: AWS::Redshift::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

allowVersionUpgrade, 유형: boolean, 기본값: true

버전 업그레이드 허용이 활성화되어 있습니다.

preferredMaintenanceWindow(선택 사항), 유형: 문자열

클러스터의 유지 관리 예약 시간입니다(예: 월요일 09:30~월요일 10:00).

automatedSnapshotRetentionPeriod(선택 사항), 유형: int, 기본값: 1

자동 스냅샷 보관 일수입니다.

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

*이러한 입력의 유효한 값에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 AutomatedSnapshotRetentionPeriod, PreferredMaintenanceWindow 및 AllowVersionUpgrade를 참조하세요.

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-cluster-multi-az-enabled

Amazon Redshift 클러스터에 여러 가용 영역 배포가 활성화되어 있는지 확인합니다. Amazon Redshift 클러스터에 여러 가용 영역 배포가 활성화되어 있지 않은 경우이 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_CLUSTER_MULTI_AZ_ENABLED

리소스 유형: AWS::Redshift::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(서울), 아시아 태평양(말레이시아), 멕시코(중부), 미국 서부(캘리포니아 북부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-cluster-parameter-group-tagged

Amazon Redshift 클러스터 파라미터 그룹에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: REDSHIFT_CLUSTER_PARAMETER_GROUP_TAGGED

리소스 유형: AWS::Redshift::ClusterParameterGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-cluster-public-access-check

Amazon Redshift 클러스터에 퍼블릭 액세스가 불가능한지 확인합니다. 클러스터 구성 항목에서 publiclyAccessible 필드가 True인 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

리소스 유형: AWS::Redshift::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-cluster-subnet-group-multi-az

Amazon Redshift 서브넷 그룹에 둘 이상의 가용 영역의 서브넷이 포함되어 있는지 확인합니다. Amazon Redshift 서브넷 그룹에 둘 이상의 다른 가용 영역의 서브넷을 포함하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_CLUSTER_SUBNET_GROUP_MULTI_AZ

리소스 유형: AWS::Redshift::ClusterSubnetGroup

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-default-admin-check

Amazon Redshift 클러스터가 관리자 사용자 이름을 기본값에서 변경했는지 확인합니다. Redshift 클러스터의 관리자 사용자 이름이 'awsuser'로 설정되어 있거나, 사용자 이름이 파라미터에 나열된 것과 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_DEFAULT_ADMIN_CHECK

리소스 유형: AWS::Redshift::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

validAdminUserNames(선택 사항), 유형: CSV

Redshift 클러스터에서 사용할 관리자 사용자 이름을 쉼표로 구분한 목록입니다. 참고로 'awsuser'가 기본값이며 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-default-db-name-check

Redshift 클러스터가 데이터베이스 이름을 기본값에서 변경했는지 확인합니다. Redshift 클러스터의 데이터베이스 이름이 'dev'로 설정되어 있거나, 선택적 파라미터가 제공되었지만 데이터베이스 이름이 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_DEFAULT_DB_NAME_CHECK

리소스 유형: AWS::Redshift::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

validDatabaseNames(선택 사항), 유형: CSV

Redshift 클러스터에 사용할 데이터베이스 이름을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-enhanced-vpc-routing-enabled

Amazon Redshift 클러스터에 'enhancedVpcRouting'이 활성화되어 있는지 확인합니다. 'enhancedVpcRouting'이 활성화되지 않았거나, configuration.enhancedVpcRouting 필드가 'false'인 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

리소스 유형: AWS::Redshift::Cluster

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-require-tls-ssl

Amazon Redshift 클러스터에서 SQL 클라이언트에 연결하기 위해 TLS/SSL 암호화가 필요한지 확인합니다. Amazon Redshift 클러스터에 true로 설정되지 않은 require_SSL 파라미터가 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_REQUIRE_TLS_SSL

리소스 유형: AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-serverless-default-admin-check

Amazon Redshift Serverless 네임스페이스가 관리자 사용자 이름을 기본값에서 변경했는지 확인합니다. Redshift Serverless 네임스페이스의 관리자 사용자 이름이 “admin”으로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_SERVERLESS_DEFAULT_ADMIN_CHECK

리소스 유형: AWS::RedshiftServerless::Namespace

트리거 유형: 주기적

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아프리카(케이프타운), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-serverless-default-db-name-check

Amazon Redshift Serverless 네임스페이스가 데이터베이스 이름을 기본값에서 변경했는지 확인합니다. Amazon Redshift Serverless 네임스페이스의 데이터베이스 이름이 `dev`로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_SERVERLESS_DEFAULT_DB_NAME_CHECK

리소스 유형: AWS::RedshiftServerless::Namespace

트리거 유형: 주기적

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아프리카(케이프타운), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-serverless-namespace-cmk-encryption

Amazon Redshift Serverless 네임스페이스가 고객 관리형 AWS KMS 키로 암호화되었는지 확인합니다. 네임스페이스가 고객 관리형 키로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다. 선택적으로 확인할 규칙에 대한 KMS 키 목록을 지정할 수 있습니다.

식별자: REDSHIFT_SERVERLESS_NAMESPACE_CMK_ENCRYPTION

리소스 유형: AWS::RedshiftServerless::Namespace

트리거 유형: 주기적

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아프리카(케이프타운), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: CSV

> 확인할 규칙에 대한 고객 관리형 키의 Amazon 리소스 이름(ARNs)을 쉼표로 구분한 목록입니다. 제공된 경우 Amazon Redshift Serverless 네임스페이스가 이러한 KMS 키 중 하나로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-serverless-publish-logs-to-cloudwatch

Amazon Redshift Serverless 네임스페이스가 다음 로그를 Amazon CloudWatch Logs에 게시하도록 구성되어 있는지 확인합니다. 네임스페이스가 Amazon CloudWatch Logs에 다음 로그를 게시하도록 구성되지 않은 경우이 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_SERVERLESS_PUBLISH_LOGS_TO_CLOUDWATCH

리소스 유형: AWS::RedshiftServerless::Namespace

트리거 유형: 주기적

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아프리카(케이프타운), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

logType(선택 사항), 유형: CSV

> CloudWatch Logs에 게시할 로그 유형의 쉼표로 구분된 목록 유효한 값은 'connectionlog', 'userlog' 기본값은 'connectionlog', 'userlog'입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-serverless-workgroup-encrypted-in-transit

AWS Redshift Serverless 작업 그룹에 require_ssl 구성 파라미터가 true로 설정되어 있는지 확인합니다. require_ssl이 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_SERVERLESS_WORKGROUP_ENCRYPTED_IN_TRANSIT

리소스 유형: AWS::RedshiftServerless::Workgroup

트리거 유형: 주기적

AWS 리전: 유럽(스톡홀름), 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부), 유럽(스페인), 유럽(취리히) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-serverless-workgroup-no-public-access

Amazon Redshift Serverless 작업 그룹이 퍼블릭 액세스를 허용하지 않는지 확인합니다. 작업 그룹에 '퍼블릭 액세스 가능 켜기'가 활성화된 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_SERVERLESS_WORKGROUP_NO_PUBLIC_ACCESS

리소스 유형: AWS::RedshiftServerless::Workgroup

트리거 유형: 주기적

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(태국), 아프리카(케이프타운), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 유럽(밀라노), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-serverless-workgroup-routes-within-vpc

Amazon Redshift Serverless 작업 그룹이 VPC를 통해 네트워크 트래픽을 라우팅하는지 확인합니다. 작업 그룹에 '향상된 VPC 라우팅 켜기'가 비활성화된 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_SERVERLESS_WORKGROUP_ROUTES_WITHIN_VPC

리소스 유형: AWS::RedshiftServerless::Workgroup

트리거 유형: 주기적

AWS 리전: 유럽(스톡홀름), 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부), 유럽(스페인), 유럽(취리히) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

redshift-unrestricted-port-access

Amazon Redshift 클러스터와 연결된 보안 그룹에 무제한 수신 트래픽을 허용하는 인바운드 규칙이 있는지 확인합니다. Redshift 클러스터 포트로의 무제한 수신 트래픽을 허용하는 인바운드 규칙이 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: REDSHIFT_UNRESTRICTED_PORT_ACCESS

리소스 유형: AWS::Redshift::Cluster

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

required-tags

리소스에 지정하는 태그가 있는지 확인합니다. 예를 들어 Amazon EC2 인스턴스에 `CostCenter` 태그가 있는지 확인하는 한편, 모든 RDS 인스턴스에 하나의 키 태그 세트가 있는지 확인할 수도 있습니다. 값이 여러 개인 경우 쉼표로 구분합니다. 한 번에 최대 6개의 태그를 검사할 수 있습니다.

AWS관리형 AWS Systems Manager 자동화 문서는이 규칙의 문제 해결로 작동하지 `AWS-SetRequiredTags` 않습니다. 문제 해결을 위해서는 사용자 지정 Systems Manager 자동화 설명서를 자체적으로 생성해야 합니다.

컨텍스트: 태그 형태로 AWS 리소스 AWS 에 메타데이터를 할당할 수 있습니다. 각 태그는 리소스에 대한 정보 또는 해당 리소스에 보관된 데이터를 저장하기 위한 키와 선택적 값으로 구성된 레이블입니다. 자세한 내용은 태그 지정 전략 구축을 참조하세요.

이 규칙을 사용하면 태그가 있어야 하는 리소스를 지정하고, 각 태그의 예상 값을 지정하여 원하는 구성으로 시작되지 않은 리소스를 내 계정에서 찾을 수 있습니다. 문제 해결 작업을 실행하여 태그 지정 실수를 수정할 수도 있습니다. 하지만 이 규칙을 사용해도 잘못된 태그가 있는 리소스를 생성하는 것을 예방하지는 못합니다.

> **Note**
>
> AWS Config 는 모든 리소스 유형에 대해 연결된 태그 기록을 지원하지 않습니다. 가 특정 리소스 유형에 대한 구성 항목(CI)에 태그를 AWS Config 기록하는지 확인하려면:
>
> - 가 태그를 제외하고 리소스에 대한 현재 구성을 AWS Config 올바르게 기록하는지 확인합니다.
> - 리소스가 변경될 때가 기록된 구성을 AWS Config 새로 고치는지 확인합니다.

식별자: REQUIRED_TAGS

리소스 유형: AWS::ACM::Certificate, AWS::AutoScaling::AutoScalingGroup, AWS::CloudFormation::Stack, AWS::CodeBuild::Project, AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkAcl, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::SecurityGroup, AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection, AWS::EC2::VPNGateway, AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup, AWS::RDS::DBSnapshot, AWS::RDS::DBSubnetGroup,

AWS::RDS::EventSubscription, AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup, AWS::Redshift::ClusterSecurityGroup, AWS::Redshift::ClusterSnapshot, AWS::Redshift::ClusterSubnetGroup, AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

tag1Key, 유형: 문자열, 기본값: CostCenter

필수 태그의 키입니다.

tag1Value(선택 사항), 유형: CSV

필수 태그의 선택적 값입니다. 값이 여러 개인 경우 쉼표로 구분합니다.

tag2Key(선택 사항), 유형: 문자열

두 번째 필수 태그의 키입니다.

tag2Value(선택 사항), 유형: CSV

두 번째 필수 태그의 선택적 값입니다. 값이 여러 개인 경우 쉼표로 구분합니다.

tag3Key(선택 사항), 유형: 문자열

세 번째 필수 태그의 키입니다.

tag3Value(선택 사항), 유형: CSV

세 번째 필수 태그의 선택적 값입니다. 값이 여러 개인 경우 쉼표로 구분합니다.

tag4Key(선택 사항), 유형: 문자열

네 번째 필수 태그의 키입니다.

tag4Value(선택 사항), 유형: CSV

네 번째 필수 태그의 선택적 값입니다. 값이 여러 개인 경우 쉼표로 구분합니다.

tag5Key(선택 사항), 유형: 문자열

다섯 번째 필수 태그의 키입니다.

tag5Value(선택 사항), 유형: CSV

다섯 번째 필수 태그의 선택적 값입니다. 값이 여러 개인 경우 쉼표로 구분합니다.

tag6Key(선택 사항), 유형: 문자열

여섯 번째 필수 태그의 키입니다.

tag6Value(선택 사항), 유형: CSV

여섯 번째 필수 태그의 선택적 값입니다. 값이 여러 개인 경우 쉼표로 구분합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

restricted-common-ports

> **Important**
>
> 이 규칙의 경우 규칙 식별자(RESTRICTED_INCOMING_TRAFFIC)와 규칙 이름(restricted-common-ports)이 서로 다릅니다.

사용 중인 보안 그룹이 지정된 포트로 TCP(Transmission Control Protocol) 트래픽의 무제한 수신을 허용하지 않는지 확인합니다. 이 규칙은 다음과 같은 경우 COMPLIANT입니다.

- 모든 TCP 트래픽에 대한 포트 액세스가 차단됩니다.
- 포트 액세스는 인바운드 규칙을 통해 TCP 트래픽에 개방됩니다. 여기에서 소스는 단일 IPv4 주소이거나, IPv4 주소를 모두 포함하지는 않는 CIDR 표기법을 된 IPv4 주소 범위('0.0.0.0/0')입니다.
- 포트 액세스는 인바운드 규칙을 통해 TCP 트래픽에 개방됩니다. 여기에서 소스는 단일 IPv6 주소이거나, IPv6 주소를 모두 포함하지는 않는 CIDR 표기법을 된 IPv6 주소 범위(‘::/0’)입니다.

인바운드 TCP 연결의 IP 주소가 지정된 포트로 제한되지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: RESTRICTED_INCOMING_TRAFFIC

리소스 유형: AWS::EC2::SecurityGroup

트리거 유형: 구성 변경 및 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

blockedPort1(선택 사항), 유형: int, 기본값: 20

차단된 TCP 포트 번호입니다. 기본값인 20은 FTP(File Transfer Protocol) 데이터 전송에 해당합니다.

blockedPort2(선택 사항), 유형: int, 기본값: 21

차단된 TCP 포트 번호입니다. 기본값인 21은 FTP(File Transfer Protocol) 명령 제어에 해당합니다.

blockedPort3(선택 사항), 유형: int, 기본값: 3389

차단된 TCP 포트 번호입니다. 기본값인 3389는 RDP(Remote Desktop Protocol)에 해당합니다.

blockedPort4(선택 사항), 유형: int, 기본값: 3306

차단된 TCP 포트 번호입니다. 기본값인 3306은 MySQL 프로토콜에 해당합니다.

blockedPort5(선택 사항), 유형: int, 기본값: 4333

차단된 TCP 포트 번호입니다. 기본값인 4333은 MySQL 프로토콜에 해당합니다.

blockedPort(선택 사항), 유형: CSV

차단된 TCP 포트 번호를 쉼표로 구분한 목록입니다. 20, 21, 3306, 3389, 4333이 그러한 예에 해당합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

root-account-hardware-mfa-enabled

AWS 계정이 다중 인증(MFA) 하드웨어 디바이스를 사용하여 루트 자격 증명으로 로그인하도록 활성화되어 있는지 확인합니다. 가상 MFA 디바이스가 루트 자격 증명을 사용하여 로그인할 수 있는 경우 규칙이 NON_COMPLIANT로 간주됩니다.

> **Note**
>
> 루트 사용자 자격 증명이 없는 계정에는 적용되지 않음
> 루트 사용자 자격 증명이 없는 `NOT_APPLICABLE` 경우이 규칙은를 반환합니다.
> 관리형 규칙 및 글로벌 IAM 리소스 유형
> 2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사

용 가능한 AWS 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 리소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에 기록할 수 없습니다. 해당 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.
주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.
불필요한 평가를 방지하려면 지원되는 리전 중 하나에만 글로벌 IAM 리소스 유형에 대해 규정 준수를 보고하는 주기적 규칙을 배포해야 합니다. 리전에서 지원되는 관리형 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.

식별자: ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

root-account-mfa-enabled

AWS 계정의 루트 사용자에게 콘솔 로그인을 위한 다중 인증이 필요한지 확인합니다. AWS Identity and Access Management(IAM) 루트 계정 사용자에게 다중 인증(MFA)이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 루트 사용자 자격 증명이 없는 계정에는 적용되지 않음
> 루트 사용자 자격 증명이 없는 `NOT_APPLICABLE` 경우이 규칙은를 반환합니다.

관리형 규칙 및 글로벌 IAM 리소스 유형
2022년 2월 이전에 온보딩된 글로벌 IAM 리소스 유형(`AWS::IAM::Group`, `AWS::IAM::Role`, 및 `AWS::IAM::User`)은 `AWS::IAM::Policy`가 2022년 2월 이전에 사용 가능한 AWS 리전에서만 AWS Config 에 의해 기록될 수 AWS Config 있습니다. 이러한 리소스 유형은 2022년 2월 AWS Config 이후에서 지원하는 리전에 기록할 수 없습니다. 해당 리전 목록은 AWS 리소스 기록 | 글로벌 리소스를 참조하세요.
주기적 규칙을 추가했던 리전에서 글로벌 IAM 리소스 유형의 기록을 활성화하지 않았더라도, 최소 하나 이상의 리전에서 글로벌 IAM 리소스 유형을 기록하는 경우, 글로벌 IAM 리소스 유형에 대한 규정 준수를 보고하는 주기적 규칙은 주기적 규칙이 추가된 모든 리전에서 평가를 실행합니다.
불필요한 평가를 방지하려면 지원되는 리전 중 하나에만 글로벌 IAM 리소스 유형에 대해 규정 준수를 보고하는 주기적 규칙을 배포해야 합니다. 리전에서 지원되는 관리형 규칙 목록은 리전 가용성별 AWS Config 관리형 규칙 목록을 참조하세요.

식별자: ROOT_ACCOUNT_MFA_ENABLED

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

route53-query-logging-enabled

Amazon Route 53 퍼블릭 호스팅 영역에서 DNS 쿼리 로깅이 활성화되어 있는지 확인합니다. Amazon Route 53 퍼블릭 호스팅 영역에서 DNS 쿼리 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: ROUTE53_QUERY_LOGGING_ENABLED

리소스 유형: AWS::Route53::HostedZone

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3express-dir-bucket-lifecycle-rules-check

Amazon S3 Express 디렉터리 버킷에 수명 주기 규칙이 구성되어 있는지 확인합니다. 활성화된 수명 주기 구성 규칙이 없거나, 구성이 파라미터 값과 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3EXPRESS_DIR_BUCKET_LIFECYCLE_RULES_CHECK

리소스 유형: AWS::S3Express::DirectoryBucket

트리거 0유형: 구성 변경

AWS 리전: 유럽(스톡홀름), 아시아 태평양(뭄바이), 미국 동부(오하이오), 유럽(아일랜드), 미국 동부(버지니아 북부), 아시아 태평양(도쿄), 미국 서부(오레곤) 리전에서만 사용 가능

파라미터:

targetExpirationDays(선택 사항), 유형: int

Amazon S3 Express 디렉터리 버킷에서 객체가 삭제된 생성 후 일수입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-access-point-in-vpc-only

Amazon S3 액세스 포인트가 인터넷에서 액세스를 허용하지 않는지 확인합니다(NetworkOrigin은 VPC). NetworkOrigin이 인터넷인 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_ACCESS_POINT_IN_VPC_ONLY

리소스 유형: AWS::S3::AccessPoint

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-access-point-public-access-blocks

Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

리소스 유형: AWS::S3::AccessPoint

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

excludedAccessPoints(선택 사항), 유형: CSV

허용된 퍼블릭 Amazon S3 액세스 포인트의 이름을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-account-level-public-access-blocks

필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 이 규칙을 사용 중인 경우, S3 퍼블릭 액세스 차단이 활성화되어 있는지 확인합니다. 규칙은 변경 트리거 규칙이므로, S3 퍼블릭 액세스 차단을 활성화하지 않는 한 호출되지 않습니다. S3 퍼블릭 액세스 차단이 활성화되지 않은 경우 규칙은 INSUFFICIENT_DATA를 반환합니다. 즉, 여전히 일부 퍼블릭 버킷이 있을 수 있습니다. S3 퍼블릭 액세스 차단 설정에 대한 자세한 내용은 Amazon S3 스토리지에 대한 퍼블릭 액세스 차단을 참조하세요.

식별자: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

리소스 유형: AWS::S3::AccountPublicAccessBlock

트리거 유형: 구성 변경(현재 상태는 확인되지 않음, 변경으로 인해 새 이벤트가 생성될 때만 평가됨)

> **Note**
>
> 이 규칙은 S3 엔드포인트가 위치한 특정 리전의 구성 변경에 의해서만 트리거됩니다. 다른 모든 리전에서는 규칙이 주기적으로 확인됩니다. 다른 리전에서 변경된 경우 규칙이 NON_COMPLIANT를 반환할 때까지 지연이 발생할 수 있습니다.

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

IgnorePublicAcls(선택 사항), 유형: 문자열, 기본값: True

IgnorePublicAcls를 적용할지 여부를 나타내며, 기본값은 True입니다.

BlockPublicPolicy(선택 사항), 유형: 문자열, 기본값: True

BlockPublicPolicy를 적용할지 여부를 나타내며, 기본값은 True입니다.

BlockPublicAcls(선택 사항), 유형: 문자열, 기본값: True

BlockPublicAcls를 적용할지 여부를 나타내며, 기본값은 True입니다.

RestrictPublicBuckets(선택 사항), 유형: 문자열, 기본값: True

RestrictPublicBuckets를 적용할지 여부를 나타내며, 기본값은 True입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-account-level-public-access-blocks-periodic

필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 구성 항목이 파라미터(또는 기본값)의 하나 이상의 설정과 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

IgnorePublicAcls(선택 사항), 유형: 문자열

IgnorePublicAcls를 적용할지 여부를 나타내며, 기본값은 True입니다.

BlockPublicPolicy(선택 사항), 유형: 문자열

BlockPublicPolicy를 적용할지 여부를 나타내며, 기본값은 True입니다.

BlockPublicAcls(선택 사항), 유형: 문자열

BlockPublicAcls를 적용할지 여부를 나타내며, 기본값은 True입니다.

RestrictPublicBuckets(선택 사항), 유형: 문자열

RestrictPublicBuckets를 적용할지 여부를 나타내며, 기본값은 True입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-acl-prohibited

Amazon Simple Storage Service(S3) 버킷이 액세스 제어 목록(ACL)을 통해 사용자 권한을 허용하는지 확인합니다. Amazon S3 버킷에서 사용자 액세스를 위해 ACL이 구성된 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_BUCKET_ACL_PROHIBITED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-blacklisted-actions-prohibited

Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대해 차단된 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 다른 AWS 계정이 버킷의 객체`s3:DeleteObject`에 대해 및 `s3:GetBucket*` 작업을 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.

> **Note**
>
> 규칙은 Principal 속성의 엔터티만 검사하며, 정책의 Condition 속성에 있는 조건부는 고려하지 않습니다.

식별자: S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(하이데라바드), 유럽(스페인) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

blacklistedActionPattern, 유형: CSV

> 예를 들어, 블랙리스트에 등록된 작업을 쉼표로 구분한 목록은 s3:GetBucket* 및 s3:DeleteObject 등의 패턴을 따릅니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-cross-region-replication-enabled

Amazon S3 버킷에 대해 S3 교차 리전 복제를 활성화했는지 확인합니다. 교차 리전 복제에 대해 활성화된 복제 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_BUCKET_CROSS_REGION_REPLICATION_ENABLED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-default-lock-enabled

S3 버킷에 기본적으로 잠금이 활성화되어 있는지 여부를 확인합니다. 잠금이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_BUCKET_DEFAULT_LOCK_ENABLED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

모드(선택 사항), 유형: 문자열

mode: (선택 사항): 유효한 값이 GOVERNANCE 또는 COMPLIANCE인 모드 파라미터입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-level-public-access-prohibited

S3 버킷이 퍼블릭 액세스 가능한지 확인합니다. S3 버킷이 `excludedPublicBuckets` 파라미터에 나열되지 않고 버킷 수준 설정이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

excludedPublicBuckets(선택 사항), 유형: CSV

알려진 허용된 퍼블릭 Amazon S3 버킷 이름을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-logging-enabled

S3 버킷에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않으면 규칙은 NON_COMPLIANT입니다.

식별자: S3_BUCKET_LOGGING_ENABLED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

targetBucket(선택 사항), 유형: 문자열

서버 액세스 로그 저장을 위한 대상 S3 버킷입니다.

targetPrefix(선택 사항), 유형: 문자열

서버 액세스 로그 저장을 위한 S3 버킷의 접두사입니다.

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
   "BucketName": "amzn-s3-demo-bucket",
   "LoggingConfiguration": {
         "DestinationBucketName": "amzn-s3-demo-destination-bucket",
         "LogFilePrefix":"my-log"
   }
}
...
```

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-mfa-delete-enabled

Amazon Simple Storage Service(S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_BUCKET_MFA_DELETE_ENABLED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-policy-grantee-check

Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 보안 AWS 주체, 페더레이션 사용자, 서비스 보안 주체, IP 주소 또는 VPCs에 의해 제한되는지 확인합니다. 버킷 정책이 없을 경우 규칙이 COMPLIANT로 간주됩니다.

예를 들어 규칙에 대한 입력 파라미터가 `111122223333`과 `444455556666`이라는 두 보안 주체 목록이고 버킷 정책에서 `111122223333`만 버킷을 액세스할 수 있도록 지정하는 경우 규칙이 COMPLIANT로 간주됩니다. 입력 파라미터가 동일하고 버킷 정책에서 `111122223333`과 `444455556666`이 버킷을 액세스할 수 있도록 지정하는 경우에도 규칙은 COMPLIANT로 간주됩니다.

하지만 버킷 정책에서 `999900009999`가 버킷을 액세스할 수 있도록 지정하는 경우에 규칙 상태는 NON-COMPLIANT입니다.

> **Note**
> 버킷 정책에 두 개 이상의 문이 포함된 경우, 버킷 정책의 각 문은 이 규칙에 따라 평가됩니다.

식별자: S3_BUCKET_POLICY_GRANTEE_CHECK

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

awsPrincipals(선택 사항), 유형: CSV

IAM 사용자 ARNs, IAM 역할 ARNs 및 AWS 계정과 같이 쉼표로 구분된 보안 주체 목록입니다. 전체 ARN을 제공하거나 부분 일치를 사용해야 합니다. 예: "arn:aws:iam::*AccountID*:role/*role_name*" 또는 "arn:aws:iam::*AccountID*:role/*". 제공된 값이 버킷 정책에 지정된 보안 주체 ARN과 정확히 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

servicePrincipals(선택 사항), 유형: CSV

서비스 보안 주체를 쉼표로 구분한 목록입니다(예: 'cloudtrail.amazonaws.com, lambda.amazonaws.com').

federatedUsers(선택 사항), 유형: CSV

웹 자격 증명 연동을 위한 자격 증명 공급자(Amazon Cognito 및 SAML 자격 증명 공급자 등)를 쉼표로 구분한 목록입니다. 그 예로 'cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider'를 들 수 있습니다.

ipAddresses(선택 사항), 유형: CSV

CIDR 형식의 IP 주소를 쉼표로 구분한 목록입니다addresses(예: '10.0.0.1, 192.168.1.0/24, 2001:db8::/32').

vpcIds(선택 사항), 유형: CSV

Amazon Virtual Private Cloud(VPC) ID를 쉼표로 구분한 목록입니다(예: 'vpc-1234abc0, vpc-ab1234c0').

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-policy-not-more-permissive

Amazon Simple Storage Service 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

> **Note**
>
> 잘못된 파라미터 값을 제공할 경우 controlPolicy 파라미터의 값은 Amazon S3 버킷 정책이어야 한다는 오류 메시지가 나타납니다.

식별자: S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

controlPolicy, 유형: 문자열

S3 버킷의 권한에 대한 상한을 정의하는 Amazon S3 버킷 정책입니다. 정책의 최대 길이는 1,024자입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-public-read-prohibited

Amazon S3 버킷이 퍼블릭 읽기 액세스를 허용하지 않는지 확인합니다. 이 규칙은 퍼블릭 액세스 차단 설정, 버킷 정책 및 버킷 액세스 제어 목록(ACL)을 확인합니다.

이 규칙은 다음 두 가지 조건을 모두 만족할 때 적용됩니다.

- 퍼블릭 액세스 차단 설정이 퍼블릭 정책을 제한하거나 버킷 정책에서 퍼블릭 읽기 액세스를 허용하지 않는 경우
- 퍼블릭 액세스 차단 설정이 퍼블릭 ACL을 제한하거나 버킷 ACL에서 퍼블릭 읽기 액세스를 허용하지 않는 경우

다음과 같은 경우 이 규칙은 적용되지 않습니다.

- 퍼블릭 액세스 차단 설정이 퍼블릭 정책을 제한하지 않는 경우는 정책이 퍼블릭 읽기 액세스를 허용하는지 AWS Config 여부를 평가합니다. 정책이 퍼블릭 읽기 액세스를 허용하는 경우 이 규칙은 적용되지 않습니다.
- 퍼블릭 액세스 차단 설정이 퍼블릭 버킷 ACLs 제한하지 않는 경우 버킷 ACL이 퍼블릭 읽기 액세스를 허용하는지 AWS Config 여부를 평가합니다. 버킷 ACL이 퍼블릭 읽기 액세스를 허용하는 경우 이 규칙은 적용되지 않습니다.

> **Note**
>
> 비공개로 간주되려면 S3 버킷 정책이 고정 값에 대한 액세스 권한만 부여해야 합니다. 즉, 와일드카드 또는 IAM 정책 요소인 변수가 포함되지 않은 값을 의미합니다.

식별자: S3_BUCKET_PUBLIC_READ_PROHIBITED

리소스 유형: AWS::S3::Bucket

트리거 유형: 구성 변경 및 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-public-write-prohibited

Amazon S3 버킷이 퍼블릭 쓰기 액세스를 허용하지 않는지 확인합니다. 이 규칙은 퍼블릭 액세스 차단 설정, 버킷 정책 및 버킷 액세스 제어 목록(ACL)을 확인합니다.

이 규칙은 다음 두 가지 조건을 모두 만족할 때 적용됩니다.

- 퍼블릭 액세스 차단 설정이 퍼블릭 정책을 제한하거나 버킷 정책에서 퍼블릭 쓰기 액세스를 허용하지 않는 경우
- 퍼블릭 액세스 차단 설정이 퍼블릭 ACL을 제한하거나 버킷 ACL에서 퍼블릭 쓰기 액세스를 허용하지 않는 경우

다음과 같은 경우 이 규칙은 적용되지 않습니다.

- 퍼블릭 액세스 차단 설정이 퍼블릭 정책을 제한하지 않는 경우는 정책이 퍼블릭 쓰기 액세스를 허용하는지 AWS Config 여부를 평가합니다. 정책이 퍼블릭 쓰기 액세스를 허용하는 경우 이 규칙은 적용되지 않습니다.
- 퍼블릭 액세스 차단 설정이 퍼블릭 버킷 ACLs 제한하지 않는 경우 버킷 ACL이 퍼블릭 쓰기 액세스를 허용하는지 AWS Config 여부를 평가합니다. 버킷 ACL이 퍼블릭 쓰기 액세스를 허용하는 경우 이 규칙은 적용되지 않습니다.

> **Note**
>
> 이 규칙은 계정 수준에서 퍼블릭 액세스 차단의 변경 사항을 평가하지 않습니다. 필수 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인하려면 s3-account-level-public-access-blocks 및 s3-account-level-public-access-blocks-periodic을 참조하세요.

> **Note**
>
> 비공개로 간주되려면 S3 버킷 정책이 고정 값에 대한 액세스 권한만 부여해야 합니다. 즉, 와일드카드 또는 IAM 정책 요소인 변수가 포함되지 않은 값을 의미합니다.

식별자: S3_BUCKET_PUBLIC_WRITE_PROHIBITED

리소스 유형: AWS::S3::Bucket

트리거 유형: 구성 변경 및 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-replication-enabled

S3 버킷에 복제 규칙이 활성화되어 있는지 확인합니다. S3 버킷에 복제 규칙이 없거나, 활성화되지 않은 복제 규칙이 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_BUCKET_REPLICATION_ENABLED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

ReplicationType(선택 사항), 유형: 문자열

> 허용되는 값은 'CROSS-REGION' 및 'SAME-REGION'입니다. 규칙에 'CROSS-REGION'을 입력하면 모든 버킷에 리전 간 복제만 활성화되어 있는지 확인할 수 있습니다. 규칙에 'SAME-REGION'을 입력하면 모든 버킷에 동일 리전 복제만 활성화되어 있는지 확인할 수 있습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-server-side-encryption-enabled

Amazon S3 버킷에 Amazon S3 기본 암호화가 활성화되어 있는지, 아니면 Amazon S3 버킷 정책이 AES-256 또는 AWS Key Management Service를 사용하는 서버 측 암호화 없이 `put-object` 요청

을 명시적으로 거부하는지 확인합니다. Amazon S3 버킷이 기본적으로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 유럽(스페인) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-ssl-requests-only

요청이 SSL/TLS를 사용하도록 요구하는 정책이 S3 버킷에 있는지 확인합니다. S3 버킷에 HTTP 요청을 허용하는 정책이 있을 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_BUCKET_SSL_REQUESTS_ONLY

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-tagged

Amazon S3 버킷에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: S3_BUCKET_TAGGED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-bucket-versioning-enabled

S3 버킷에 버전 관리가 활성화되어 있는지 확인합니다. 이 규칙은 필요에 따라 S3 버킷에 MFA 삭제가 활성화되어 있는지 확인합니다.

식별자: S3_BUCKET_VERSIONING_ENABLED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

isMfaDeleteEnabled(선택 사항), 유형: 문자열

S3 버킷에 MFA 삭제가 활성화되어 있습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-default-encryption-kms

S3 버킷이 AWS Key Management Service(AWS KMS)로 암호화되었는지 확인합니다. S3 버킷이 AWS KMS 키로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_DEFAULT_ENCRYPTION_KMS

리소스 유형: AWS::S3::Bucket, AWS::KMS::Key

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: CSV

Amazon S3 버킷 암호화에 허용되는 AWS KMS 키 ARNs의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-event-notifications-enabled

Amazon S3 이벤트 알림이 S3 버킷에 대해 활성화되어 있는지 확인합니다. S3 이벤트 알림이 버킷에 대해 설정되어 있지 않거나, 이벤트 유형 또는 대상이 `eventTypes` 및 destinationArn 파라미터와 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_EVENT_NOTIFICATIONS_ENABLED

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

destinationArn(선택 사항), 유형: 문자열

이벤트 알림 대상의 Amazon 리소스 이름(ARN)입니다(Amazon SNS 주제, AWS Lambda, Amazon SQS 대기열).

eventTypes(선택 사항), 유형: CSV

기본 Amazon S3 이벤트 유형을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-last-backup-recovery-point-created

Amazon Simple Storage Service(S3)에 대한 복구 시점이 생성되었는지 확인합니다. 지정된 기간 내에 생성된 해당하는 복구 시점이 Amazon S3 버킷에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_LAST_BACKUP_RECOVERY_POINT_CREATED

리소스 유형: AWS::S3::Bucket

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon S3 버킷의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon S3 버킷의 이름입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 744시간, 일수는 31일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-lifecycle-policy-check

수명 주기 규칙이 Amazon Simple Storage Service(S3) 버킷에 구성되어 있는지 확인합니다. 활성화된 수명 주기 구성 규칙이 없거나, 구성이 파라미터 값과 일치하지 않는 경우 규칙은 NON_COMPLIANT 입니다.

식별자: S3_LIFECYCLE_POLICY_CHECK

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

targetTransitionDays(선택 사항), 유형: int

객체 생성 후 객체를 지정된 스토리지 클래스로 전환하는 시기까지의 일수입니다(예: 30일).

targetExpirationDays(선택 사항), 유형: int

객체 생성 후 객체가 삭제되는 일수입니다(예: 395일).

targetTransitionStorageClass(선택 사항), 유형: 문자열

대상 스토리지 클래스 유형입니다. Amazon S3 Standard-Infrequent Access(S3 Standard-IA)를 예로 들 수 있습니다. 자세한 내용은 Amazon S3 스토리지 클래스 이해 및 관리를 참조하세요.

targetPrefix(선택 사항), 유형: 문자열

Amazon S3 객체 접두사는 하나 이상의 객체를 식별할 수 있습니다.

bucketNames(선택 사항), 유형: CSV

수명 주기 정책이 활성화된 Amazon S3 버킷 이름을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-meets-restore-time-target

Amazon Simple Storage Service(S3) 버킷의 복원 시간이 지정된 기간을충족하는지 확인합니다. Amazon S3 버킷의 LatestRestoreExecutionTimeMinutes가 maxRestoreTime(분)보다 큰 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_MEETS_RESTORE_TIME_TARGET

리소스 유형: AWS::S3::Bucket

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

maxRestoreTime, 유형: int

허용되는 최대 복원 런타임의 숫자 값입니다.

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon S3 버킷의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon S3 버킷의 이름입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-resources-in-logically-air-gapped-vault

Amazon Simple Storage Service(Amazon S3) 버킷이 논리적 에어 갭 저장소에 있는지 확인합니다. Amazon S3 버킷이 지정된 기간 내에 논리적 에어 갭 저장소에 없는 경우 규칙은 NON_COMPLIANT 입니다.

식별자: S3_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

리소스 유형: AWS::S3::Bucket

트리거 유형: 주기적

AWS 리전: 유럽(스톡홀름), 중동(바레인), 아시아 태평양(뭄바이), 유럽(파리), 미국 동부(오하이오), 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 아시아 태평양(서울), 아시아 태평양(오사카), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부) 리전에서만 사용 가능

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon S3 버킷의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon S3 버킷의 이름입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 2184시간, 일수는 91일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-resources-protected-by-backup-plan

Amazon Simple Storage Service(S3) 버킷이 백업 플랜에 의해 보호되는지 확인합니다. Amazon S3 버킷을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

리소스 유형: AWS::S3::Bucket

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon S3 버킷의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Amazon S3 버킷의 이름입니다.

crossRegionList(선택 사항), 유형: 문자열

리전 간 백업 사본을 보관할 대상 리전을 쉼표로 구분한 목록입니다.

crossAccountList(선택 사항), 유형: 문자열

계정 간 백업 사본을 보관할 대상 계정을 쉼표로 구분한 목록입니다.

maxRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최대 보존 기간(일)

minRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최소 보존 기간(일)

backupVaultLockCheck(선택 사항), 유형: 문자열

허용되는 값: 'True' 또는 'False'. 리소스가 잠긴 볼트에 백업되어 있는지 확인하는 규칙에 'True'를 입력합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

s3-version-lifecycle-policy-check

Amazon Simple Storage Service(S3) 버전 지원 버킷에 수명 주기 정책이 구성되어 있는지 확인합니다. Amazon S3 수명 주기 정책이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: S3_VERSION_LIFECYCLE_POLICY_CHECK

리소스 유형: AWS::S3::Bucket

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

bucketNames(선택 사항), 유형: CSV

수명 주기 정책이 활성화된 Amazon S3 버킷 이름을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-app-image-config-tagged

Amazon SageMaker 앱 이미지 구성에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: SAGEMAKER_APP_IMAGE_CONFIG_TAGGED

리소스 유형: AWS::SageMaker::AppImageConfig

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-domain-in-vpc

Amazon SageMaker 도메인이 고객 소유의 Amazon Virtual Private Cloud(VPC)를 비 EFS 트래픽에 사용하는지 확인합니다. configuration.AppNetworkAccessType이 VpcOnly로 설정되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: SAGEMAKER_DOMAIN_IN_VPC

리소스 유형: AWS::SageMaker::Domain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-domain-tagged

Amazon SageMaker 도메인에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: SAGEMAKER_DOMAIN_TAGGED

리소스 유형: AWS::SageMaker::Domain

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-endpoint-configuration-kms-key-configured

AWS Key Management Service(AWS KMS) 키가 Amazon SageMaker 엔드포인트 구성에 대해 구성되어 있는지 확인합니다. Amazon SageMaker 엔드포인트 구성에 'KmsKeyId'가 지정되지 않은 경우 규칙은 NON_COMPLIANT입니다.

Identifier: SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

리소스 유형: AWS::SageMaker::EndpointConfig

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: 문자열

Amazon SageMaker 엔드포인트 구성에 허용되는 특정 AWS KMS 키 ARNs의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-endpoint-config-prod-instance-count

Amazon SageMaker 엔드포인트 구성에 프로덕션 변형 `InitialInstanceCount`가 1보다 큰 값으로 설정되어 있는지 확인합니다. 프로덕션 변형 `InitialInstanceCount`가 1인 경우 규칙은 NON_COMPLIANT입니다.

식별자: SAGEMAKER_ENDPOINT_CONFIG_PROD_INSTANCE_COUNT

리소스 유형: AWS::SageMaker::EndpointConfig

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-feature-group-tagged

Amazon SageMaker 특성 그룹에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: SAGEMAKER_FEATURE_GROUP_TAGGED

리소스 유형: AWS::SageMaker::FeatureGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-image-description

Amazon SageMaker 이미지에 설명이 있는지 확인합니다. configuration.ImageDescription이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: SAGEMAKER_IMAGE_DESCRIPTION

리소스 유형: AWS::SageMaker::Image

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-image-tagged

Amazon SageMaker 이미지에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: SAGEMAKER_IMAGE_TAGGED

리소스 유형: AWS::SageMaker::Image

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-model-in-vpc

Amazon SageMaker 모델이 컨테이너 트래픽에 Amazon Virtual Private Cloud(VPC)를 사용하는지 확인합니다. configuration.VpcConfig가 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: SAGEMAKER_MODEL_IN_VPC

리소스 유형: AWS::SageMaker::Model

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-model-isolation-enabled

Amazon SageMaker 모델에 네트워크 격리가 활성화되어 있는지 확인합니다. configuration.EnableNetworkIsolation이 false인 경우 규칙은 NON_COMPLIANT입니다.

식별자: SAGEMAKER_MODEL_ISOLATION_ENABLED

리소스 유형: AWS::SageMaker::Model

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-notebook-instance-inside-vpc

Amazon SageMaker 노트북 인스턴스가 VPC 내에서 시작되었는지 또는 승인된 서브넷 목록 내에서 시작되었는지 확인합니다. 노트북 인스턴스가 VPC 내에서 시작되지 않았거나, 해당 서브넷 ID가 파라미터 목록에 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

리소스 유형: AWS::SageMaker::NotebookInstance

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

SubnetIds(선택 사항), 유형: CSV

노트북 인스턴스를 시작할 수 있는 서브넷 ID를 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-notebook-instance-kms-key-configured

Amazon SageMaker 노트북 인스턴스에 대해 AWS Key Management Service(AWS KMS) 키가 구성되어 있는지 확인합니다. 'KmsKeyId'가 SageMaker 노트북 인스턴스에 대해 지정되지 않으면 규칙은 NON_COMPLIANT입니다.

식별자: SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

리소스 유형: AWS::SageMaker::NotebookInstance

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: 문자열

Amazon SageMaker 노트북 인스턴스에 허용되는 AWS KMS 키 ARNs의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-notebook-instance-platform-version

지원되는 플랫폼 식별자 버전을 사용하도록 Sagemaker 노트북 인스턴스가 구성되어 있는지 확인합니다. 노트북 인스턴스가 파라미터에 지정된 지원되는 플랫폼 식별자 버전을 사용하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: SAGEMAKER_NOTEBOOK_INSTANCE_PLATFORM_VERSION

리소스 유형: AWS::SageMaker::NotebookInstance

트리거 유형: 주기적

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

supportedPlatformIdentifierVersions, 유형: CSV

확인할 규칙에 대해 지원되는 플랫폼 식별자 버전의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-notebook-instance-root-access-check

Amazon SageMaker RootAccess 설정이 Amazon SageMaker 노트북 인스턴스에 대해 활성화되어 있는지 확인합니다. Amazon SageMaker 노트북 인스턴스에 대해 RootAccess 설정이 'Enabled'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

식별자: SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

리소스 유형: AWS::SageMaker::NotebookInstance

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sagemaker-notebook-no-direct-internet-access

직접 인터넷 액세스가 Amazon SageMaker 노트북 인스턴스에 대해 비활성화되어 있는지 확인합니다. SageMaker 노트북 인스턴스에서 인터넷이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

리소스 유형: AWS::SageMaker::NotebookInstance

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

secretsmanager-rotation-enabled-check

AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 이 규칙은 선택적 `maximumAllowedRotationFrequency` 파라미터도 확인합니다. 파라미터가 지정되면 보안 암호의 교체 빈도가 허용되는 최대 빈도와 비교됩니다. 보안 암호의 교체가 예약되지 않은 경우 규칙은 NON_COMPLIANT입니다. 교체 빈도가 maximumAllowedRotationFrequency 파라미터에 지정된 숫자보다 높은 경우에도 규칙은 NON_COMPLIANT가 됩니다.

> **Note**
>
> 첫 번째 평가 후 4시간 이내에 이 규칙을 재평가하는 것은 결과에 아무런 영향을 주지 않습니다.

식별자: SECRETSMANAGER_ROTATION_ENABLED_CHECK

리소스 유형: AWS::SecretsManager::Secret

트리거 0유형: 구성 변경

AWS 리전: 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

maximumAllowedRotationFrequency(선택 사항), 유형: int

보안 암호의 최대 허용 교체 빈도(일)입니다.

maximumAllowedRotationFrequencyInHours(선택 사항), 유형: int

보안 암호의 최대 허용 교체 빈도(시간)입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

secretsmanager-scheduled-rotation-success-check

AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 레코딩 지연
>
> 이 규칙에 대한 평가 결과는 교체 누락일로부터 최대 2일까지 지연될 수 있습니다. 보다 즉각적인 모니터링은 Secrets Manager 사용 설명서의 Amazon CloudWatch로 AWS Secrets Manager 모니터링을 참조하세요.
>
> 교체 없는 보안 암호
>
> 규칙은 교체`NOT_APPLICABLE`하도록 구성되지 않은 보안 암호에 대해를 반환합니다.

식별자: SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

리소스 유형: AWS::SecretsManager::Secret

트리거 0유형: 구성 변경

AWS 리전: 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

secretsmanager-secret-periodic-rotation

AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

식별자: SECRETSMANAGER_SECRET_PERIODIC_ROTATION

리소스 유형: AWS::SecretsManager::Secret

트리거 유형: 주기적

AWS 리전: 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

maxDaysSinceRotation(선택 사항), 유형: int

보안 암호를 변경하지 않은 상태로 유지할 수 있는 최대 일수입니다. 기본값은 90일입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

secretsmanager-secret-unused

지정된 일수 내에 AWS Secrets Manager 보안 암호에 액세스했는지 확인합니다. 'unusedForDays' 일수 내에 보안 암호에 액세스하지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

컨텍스트: 사용하지 않는 보안 암호는 정기적으로 삭제하는 것이 좋습니다. 이러한 보안 암호에 더 이상 액세스할 필요가 없는 이전 사용자가 사용하지 않는 보안 암호를 남용할 우려가 있습니다. 또한 보안 암호에 액세스할 수 있는 사용자가 많아질수록 누군가가 보안 암호를 남용하거나, 승인되지 않은 엔터티에 대한 액세스 권한을 부여할 가능성이 한층 더 커집니다. 사용하지 않는 보안 암호를 삭제하면 해당 암호가 더 이상 필요하지 않은 사용자로부터 암호 액세스 권한을 취소할 수 있으며, AWS Secrets Manager사용 비용도 줄일 수 있습니다.

식별자: SECRETSMANAGER_SECRET_UNUSED

리소스 유형: AWS::SecretsManager::Secret

트리거 유형: 주기적

AWS 리전: 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

unusedForDays(선택 사항), 유형: int

보안 암호를 사용하지 않은 상태로 유지할 수 있는 일수입니다. 기본값은 90일입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

secretsmanager-using-cmk

의 모든 보안 암호 AWS Secrets Manager 가 AWS 관리형 키 (`aws/secretsmanager`) 또는 AWS Key Management Service ()에서 생성된 고객 관리형 키를 사용하여 암호화되었는지 확인합니다AWS KMS. 고객 관리형 키를 사용하여 보안 암호를 암호화하는 경우 규칙은 COMPLIANT입니다. `aws/secretsmanager`를 사용하여 암호를 암호화한 경우 이 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 이 규칙은 교차 계정 고객 관리형 키에 대한 액세스 권한이 없으며, 교차 계정 키가 사용될 경우 보안 암호를 NON_COMPLIANT로 평가합니다.

식별자: SECRETSMANAGER_USING_CMK

리소스 유형: AWS::SecretsManager::Secret

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

kmsKeyArns(선택 사항), 유형: CSV

암호화에 키가 사용되었는지 확인하기 위한 KMS 키 Amazon 리소스 이름(ARN)을 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

securityhub-enabled

AWS 계정에 대해 AWS Security Hub가 활성화되어 있는지 확인합니다. AWS Security Hub가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: SECURITYHUB_ENABLED

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

security-account-information-provided

AWS 계정 연락처에 대한 보안 연락처 정보를 제공했는지 확인합니다. 계정 내에 보안 연락처 정보가 제공되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: SECURITY_ACCOUNT_INFORMATION_PROVIDED

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

service-catalog-shared-within-organization

AWS Organizations와의 통합이 활성화된 경우 AWS Service Catalog가 조직(단일 단위로 취급되는 AWS 계정 모음)과 포트폴리오를 공유하는지 확인합니다. 공유의 `Type` 값이 `ACCOUNT`인 경우 규칙은 NON_COMPLIANT입니다.

식별자: SERVICE_CATALOG_SHARED_WITHIN_ORGANIZATION

리소스 유형: AWS::ServiceCatalog::Portfolio

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

service-vpc-endpoint-enabled

규칙 파라미터에 제공된 서비스의 서비스 엔드포인트가 각 Amazon Virtual Private Cloud(VPC)에 대해 생성되었는지 확인합니다. 서비스에 대해 생성된 Amazon VPC 엔드포인트가 Amazon VPC에 없는 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: SERVICE_VPC_ENDPOINT_ENABLED

리소스 유형: AWS::EC2::VPC

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

serviceName, 유형: 문자열

> 서비스의 짧은 이름 또는 접미사입니다. 참고로, 사용 가능한 서비스 이름 목록 또는 유효한 접미사 목록을 가져오려면 DescribeVpcEndpointServices를 사용하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ses-malware-scanning-enabled

Amazon Simple Email Service(Amazon SES)에 대해 메시지 수신 시 멀웨어 및 스팸 스캔이 활성화되어 있는지 확인합니다. 멀웨어 및 스팸 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: SES_MALWARE_SCANNING_ENABLED

리소스 유형: AWS::SES::ReceiptRule

트리거 유형: 주기적

AWS 리전: 유럽(아일랜드), 미국 동부(버지니아 북부), 미국 서부(오레곤) 리전에서만 사용 가능합니다.

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

shield-advanced-enabled-autorenew

AWS 계정에서 AWS Shield Advanced가 활성화되어 있고이 구독이 자동으로 갱신되도록 설정되어 있는지 확인합니다. Shield Advanced가 활성화되어 있고 자동 갱신이 활성화된 경우 규칙은 COMPLIANT입니다.

> **Note**
>
> 의 API 엔드포인트 AWS Shield Advanced 는 미국 동부(버지니아 북부) 리전에서만 사용할 수 있습니다. 이 규칙은 미국 동부(버지니아 북부) 리전에서만 실행되도록 예약해야 합니다.

식별자: SHIELD_ADVANCED_ENABLED_AUTORENEW

트리거 유형: 주기적

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

shield-drt-access

Shield 대응 팀(SRT)이 AWS 계정에 액세스할 수 있는지 확인합니다. 이 AWS Shield Advanced 활성화되었지만 SRT 액세스에 대한 역할이 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: SHIELD_DRT_ACCESS

트리거 유형: 주기적

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sns-encrypted-kms

SNS 주제가 AWS Key Management Service(AWS KMS)로 암호화되었는지 확인합니다. SNS 주제가 AWS KMS로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다. 필요에 따라 확인할 규칙의 주요 ARN, 별칭 ARN, 별칭 이름 또는 키 ID를 지정합니다.

식별자: SNS_ENCRYPTED_KMS

리소스 유형: AWS::SNS::Topic

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

kmsKeyIds(선택 사항), 유형: CSV

> 확인할 규칙에 대한 AWS KMS 키 Amazon 리소스 이름(ARNs), KMS 별칭 ARNs, KMS 별칭 이름 또는 KMS 키 IDs의 쉼표로 구분된 목록입니다.

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
}
...
```

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sns-topic-message-delivery-notification-enabled

엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

리소스 유형: AWS::SNS::Topic

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sns-topic-no-public-access

SNS 주제 액세스 정책이 퍼블릭 액세스를 허용하는지 확인합니다. SNS 주제 액세스 정책이 퍼블릭 액세스를 허용하는 경우 이 규칙은 NON_COMPLIANT입니다.

> **Note**
> 비공개로 간주되려면 SNS 정책이 고정 값에 대한 액세스 권한만 부여해야 합니다. 즉, 와일드카드 또는 IAM 정책 요소인 변수가 포함되지 않은 값을 의미합니다.

식별자: SNS_TOPIC_NO_PUBLIC_ACCESS

리소스 유형: AWS::SNS::Topic

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

sqs-queue-no-public-access

SQS 대기열 액세스 정책이 퍼블릭 액세스를 허용하는지 확인합니다. SQS 대기열 액세스 정책이 퍼블릭 액세스를 허용하는 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
> 비공개로 간주되려면 SQS 정책이 고정 값에 대한 액세스 권한만 부여해야 합니다. 즉, 와일드카드 또는 IAM 정책 요소인 변수가 포함되지 않은 값을 의미합니다.

식별자: SQS_QUEUE_NO_PUBLIC_ACCESS

리소스 유형: AWS::SQS::Queue

트리거 0유형: 구성 변경

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ssm-automation-block-public-sharing

AWS Systems Manager Automation에 퍼블릭 공유 차단이 활성화되어 있는지 확인합니다. Systems Manager Automation에 퍼블릭 공유 차단이 비활성화된 경우 규칙은 NON_COMPLIANT입니다.

식별자: SSM_AUTOMATION_BLOCK_PUBLIC_SHARING

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(서울), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ssm-automation-logging-enabled

AWS Systems Manager Automation에 Amazon CloudWatch 로깅이 활성화되어 있는지 확인합니다. Systems Manager Automation에 CloudWatch 로깅이 활성화되지 않은 경우 규칙은 NON_COMPLIANT를 반환합니다.

식별자: SSM_AUTOMATION_LOGGING_ENABLED

리소스 유형: AWS::::Account

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(서울), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ssm-document-not-public

계정이 소유한 AWS Systems Manager 문서가 공개되어 있는지 확인합니다. 소유자가 '본인'인 Systems Manager 문서가 공개되어 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: SSM_DOCUMENT_NOT_PUBLIC

리소스 유형: AWS::SSM::Document

트리거 유형: 주기적

AWS 리전: 아시아 태평양(타이베이), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

ssm-document-tagged

AWS Systems Manager 문서에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: SSM_DOCUMENT_TAGGED

리소스 유형: AWS::SSM::Document

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

step-functions-state-machine-logging-enabled

AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

식별자: STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

리소스 유형: AWS::StepFunctions::StateMachine

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

cloudWatchLogGroupArns(선택 사항), 유형: CSV

Amazon CloudWatch Logs 로그 그룹에 대한 Amazon 리소스 이름(ARN)을 쉼표로 구분한 목록입니다. 규칙은 상태 시스템 로그에 대해 지정된 로그 그룹이 구성되어 있는지 확인합니다.

logLevel(선택 사항), 유형: 문자열

상태 시스템의 최소 로그 수준입니다. 유효한 값에는 ALL, ERROR, FATAL이 포함됩니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

storagegateway-last-backup-recovery-point-created

AWS Storage Gateway 볼륨에 대한 복구 시점이 생성되었는지 확인합니다. 지정된 기간 내에 생성된 해당하는 복구 시점이 Storage Gateway 볼륨에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED

리소스 유형: AWS::StorageGateway::Volume

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Storage Gateway 볼륨의 태그입니다(JSON 형식`{"tagkey" : "tagValue"}`).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Storage Gateway 볼륨의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 744시간, 일수는 31일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

storagegateway-resources-in-logically-air-gapped-vault

AWS Storage Gateway 볼륨이 논리적 에어 갭 저장소에 있는지 확인합니다. 지정된 기간 내에 AWS Storage Gateway 볼륨이 논리적 에어 갭 저장소에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: STORAGEGATEWAY_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

리소스 유형: AWS::StorageGateway::Volume

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Storage Gateway 볼륨의 태그(JSON 형식)

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Storage Gateway 볼륨의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 2184시간, 일수는 91일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

storagegateway-resources-protected-by-backup-plan

AWS Storage Gateway 볼륨이 백업 계획으로 보호되는지 확인합니다. Storage Gateway 볼륨을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

리소스 유형: AWS::StorageGateway::Volume

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 Storage Gateway 볼륨의 태그입니다(JSON 형식).

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 Storage Gateway 볼륨의 ID입니다.

crossRegionList(선택 사항), 유형: 문자열

리전 간 백업 사본을 보관할 대상 리전을 쉼표로 구분한 목록입니다.

crossAccountList(선택 사항), 유형: 문자열

계정 간 백업 사본을 보관할 대상 계정을 쉼표로 구분한 목록입니다.

maxRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최대 보존 기간(일)

minRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최소 보존 기간(일)

backupVaultLockCheck(선택 사항), 유형: 문자열

허용되는 값: 'True' 또는 'False'. 리소스가 잠긴 볼트에 백업되어 있는지 확인하는 규칙에 'True'를 입력합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

subnet-auto-assign-public-ip-disabled

Amazon Virtual Private Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 할당되어 있는지 확인합니다. Amazon VPC에 퍼블릭 IP 주소가 할당된 서브넷이 없는 경우 규칙은 COMPLIANT입니다. Amazon VPC에 퍼블릭 IP 주소가 할당된 서브넷이 있는 경우 규칙은 NON_COMPLIANT입니다.

식별자: SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

리소스 유형: AWS::EC2::Subnet

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

사전 평가

사전 예방 모드에서이 규칙을 실행하는 방법에 대한 단계는 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 이 규칙이 사전 예방 모드에서 COMPLIANT를 반환하려면 StartResourceEvaluation API의 리소스 구성 스키마에 문자열로 인코딩된 다음과 같은 입력을 포함해야 합니다.

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

사전 평가에 대한 자세한 내용은 평가 모드를 참조하세요.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

transfer-agreement-description

AWS Transfer Family 계약에 설명이 있는지 확인합니다. configuration.Description이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: TRANSFER_AGREEMENT_DESCRIPTION

리소스 유형: AWS::Transfer::Agreement

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

transfer-agreement-tagged

AWS Transfer Family 계약에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: TRANSFER_AGREEMENT_TAGGED

리소스 유형: AWS::Transfer::Agreement

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

transfer-certificate-description

AWS Transfer Family 인증서에 설명이 있는지 확인합니다. configuration.Description이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: TRANSFER_CERTIFICATE_DESCRIPTION

리소스 유형: AWS::Transfer::Certificate

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

transfer-certificate-tagged

AWS Transfer Family 인증서에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: TRANSFER_CERTIFICATE_TAGGED

리소스 유형: AWS::Transfer::Certificate

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

transfer-connector-logging-enabled

AWS Transfer Family Connector가 Amazon CloudWatch에 로그를 게시하는지 확인합니다. 커넥터에 LoggingRole이 할당되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: TRANSFER_CONNECTOR_LOGGING_ENABLED

리소스 유형: AWS::Transfer::Connector

트리거 0유형: 구성 변경

AWS 리전: 중동(바레인), 아시아 태평양(태국), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

transfer-connector-tagged

AWS Transfer Family 커넥터에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: TRANSFER_CONNECTOR_TAGGED

리소스 유형: AWS::Transfer::Connector

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

transfer-family-server-no-ftp

AWS Transfer Family로 생성된 서버가 엔드포인트 연결에 FTP를 사용하는지 확인합니다. 엔드포인트 연결을 위한 서버 프로토콜이 FTP를 활성화한 경우 규칙은 NON_COMPLIANT입니다.

식별자: TRANSFER_FAMILY_SERVER_NO_FTP

리소스 유형: AWS::Transfer::Server

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

transfer-profile-tagged

AWS Transfer Family 프로필에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: TRANSFER_PROFILE_TAGGED

리소스 유형: AWS::Transfer::Profile

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

transfer-workflow-description

AWS Transfer Family 워크플로에 설명이 있는지 확인합니다. configuration.Description이 없거나 빈 문자열인 경우 규칙은 NON_COMPLIANT입니다.

식별자: TRANSFER_WORKFLOW_DESCRIPTION

리소스 유형: AWS::Transfer::Workflow

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

transfer-workflow-tagged

AWS Transfer Family 워크플로에 태그가 있는지 확인합니다. 선택적으로 태그 키를 지정할 수 있습니다. 태그가 없거나 지정된 태그 키가 없는 경우 규칙은 NON_COMPLIANT입니다. 규칙은 'aws:'로 시작하는 태그를 확인하지 않습니다.

식별자: TRANSFER_WORKFLOW_TAGGED

리소스 유형: AWS::Transfer::Workflow

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

requiredKeyTags(선택 사항), 유형: CSV

> 확인할 규칙에 대한 태그 키의 쉼표로 구분된 목록입니다. 제공된 경우 평가된 리소스에 이러한 키가 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다. 태그 키는 대/소문자를 구분합니다. 'aws:'로 시작하는 태그 키는 허용되지 않습니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

virtualmachine-last-backup-recovery-point-created

AWS Backup-Gateway VirtualMachines에 대한 복구 시점이 생성되었는지 확인합니다. AWS Backup-Gateway VirtualMachines에 지정된 기간 내에 생성된 해당 복구 시점이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

리소스 유형: AWS::BackupGateway::VirtualMachine

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 AWS Backup-Gateway VirtualMachines의 태그로, JSON 형식입니다`{"tagkey" : "tagValue"}`.

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 AWS Backup-Gateway VirtualMachine의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 744시간, 일수는 31일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

virtualmachine-resources-in-logically-air-gapped-vault

AWS Backup-Gateway VirtualMachines가 논리적 에어 갭 저장소에 있는지 확인합니다. AWS Backup-Gateway VirtualMachines가 지정된 기간 내에 논리적 에어 갭 저장소에 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: VIRTUALMACHINE_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

리소스 유형: AWS::BackupGateway::VirtualMachine

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 AWS Backup-Gateway VirtualMachines의 태그로, JSON 형식입니다.

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 AWS Backup-Gateway VirtualMachine의 ID입니다.

recoveryPointAgeValue(선택 사항), 유형: int, 기본값: 1

허용되는 최대 수명의 숫자 값입니다. 시간은 2184시간, 일수는 91일을 넘지 않아야 합니다.

recoveryPointAgeUnit(선택 사항), 유형: 문자열, 기본값: 일

허용되는 최대 수명의 시간 단위입니다. 허용되는 값: '시간', '일'.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

virtualmachine-resources-protected-by-backup-plan

AWS Backup-Gateway VirtualMachines가 백업 계획으로 보호되는지 확인합니다. Backup-Gateway VirtualMachine을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

식별자: VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

리소스 유형: AWS::BackupGateway::VirtualMachine

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), 멕시코(중부), 이스라엘(텔아비

브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

resourceTags(선택 사항), 유형: 문자열

확인할 규칙에 대한 AWS Backup-Gateway VirtualMachines의 태그로, JSON 형식입니다`{"tagkey" : "tagValue"}`.

resourceId(선택 사항), 유형: 문자열

확인할 규칙에 대한 AWS Backup-Gateway VirtualMachine의 ID입니다.

crossRegionList(선택 사항), 유형: 문자열

리전 간 백업 사본을 보관할 대상 리전을 쉼표로 구분한 목록입니다.

crossAccountList(선택 사항), 유형: 문자열

계정 간 백업 사본을 보관할 대상 계정을 쉼표로 구분한 목록입니다.

maxRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최대 보존 기간(일)

minRetentionDays(선택 사항), 유형: int

백업 볼트 잠금의 최소 보존 기간(일)

backupVaultLockCheck(선택 사항), 유형: 문자열

허용되는 값: 'True' 또는 'False'. 리소스가 잠긴 볼트에 백업되어 있는지 확인하는 규칙에 'True'를 입력합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

vpc-default-security-group-closed

Amazon Virtual Private Cloud(VPC)의 기본 보안 그룹이 인바운드 또는 아웃바운드 트래픽을 허용하지 않는지 확인합니다. 기본 보안 그룹에 하나 이상의 인바운드 또는 아웃바운드 트래픽 규칙이 있는 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 가 Amazon VPC 삭제의 일부로 삭제되는 기본 보안 그룹과 같은 관련 리소스의 삭제를 AWS Config 기록하는 시점 사이에 지연이 있을 수 있습니다. 따라서 모든 기본 보안 그룹 또는 기타 관련 리소스가 삭제되거나 수정되더라도, 다음 계정 기준 설정 프로세스가 완료될 때까지 규칙은 NON_COMPLIANT를 보고할 수도 있습니다.

식별자: VPC_DEFAULT_SECURITY_GROUP_CLOSED

리소스 유형: AWS::EC2::SecurityGroup

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

vpc-endpoint-enabled

파라미터에 지정된 각 서비스에 Amazon VPC 엔드포인트가 있는지 확인합니다. 지정한 각 서비스에 대해 생성된 VPC 엔드포인트가 Amazon VPC에 없는 경우 이 규칙은 NON_COMPLIANT입니다. 필요한 경우, 확인할 규칙의 특정 VPC를 지정할 수 있습니다.

식별자: VPC_ENDPOINT_ENABLED

리소스 유형: AWS::EC2::VPC

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 아시아 태평양(오사카), 아시아 태평양(말레이시아), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

serviceNames, 유형: CSV

서비스 이름 또는 엔드포인트의 쉼표로 구분된 목록입니다. 예: "access-analyzer, appconfig, cloudtrail" 또는 "com.amazonaws.region.access-analyzer" 사용 가능한 이름은 DescribeVpcEndpointServices를 사용합니다.

vpcIds(선택 사항), 유형: CSV

VPC 엔드포인트용 Amazon VPC ID의 쉼표로 구분된 목록입니다. serviceName 파라미터에 지정된 서비스에 이러한 VPC 엔드포인트 중 하나가 없는 경우 규칙은 NON_COMPLIANT입니다.

scopeConfigResourceTypes(선택 사항), 유형: CSV

확인할 규칙에 대한 AWS Config 리소스 유형의 쉼표로 구분된 목록입니다. 지정된 경우 규칙은 계정에 지정된 리소스가 하나 이상 기록된 경우에만 규정 준수 상태를 반환합니다. 예: "AWS::SNS::Topic".

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

vpc-flow-logs-enabled

모든 Amazon VPC에 대해 Amazon Virtual Private Cloud(VPC) 흐름 로그가 검색되고 활성화되어 있는지 확인합니다. 하나 이상의 Amazon VPC에 대해 흐름 로그가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: VPC_FLOW_LOGS_ENABLED

리소스 유형: AWS::EC2::VPC

트리거 유형: 주기적

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

trafficType(선택 사항), 유형: 문자열

흐름 로그의 TrafficType

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

vpc-network-acl-unused-check

사용하지 않는 네트워크 액세스 제어 목록(네트워크 ACL)이 있는지 확인합니다. 각 네트워크 ACL이 서브넷과 연결되어 있는 경우 규칙은 COMPLIANT입니다. 네트워크 ACL이 서브넷과 연결되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: VPC_NETWORK_ACL_UNUSED_CHECK

리소스 유형: AWS::EC2::NetworkAcl

트리거 0유형: 구성 변경

AWS 리전: 지원되는 모든 AWS 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

vpc-peering-dns-resolution-check

수락자/요청자 VPC에서 프라이빗 IP로의 DNS 확인이 활성화되어 있는지 확인합니다. 수락자/요청자 VPC에서 프라이빗 IP로의 DNS 확인이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: VPC_PEERING_DNS_RESOLUTION_CHECK

리소스 유형: AWS::EC2::VPCPeeringConnection

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

vpcIds(선택 사항), 유형: CSV

확인할 VPC를 쉼표로 구분한 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

vpc-sg-open-only-to-authorized-ports

무제한 수신 트래픽('0.0.0.0/0' 또는 '::/0')을 허용하는 보안 그룹이 승인된 포트의 인바운드 TCP 또는 UDP 연결만 허용하는지 확인합니다. 이러한 보안 그룹에 규칙 파라미터에 지정된 포트가 없을 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> 이 규칙은 수신 규칙이 IPv4='0.0.0.0/0' 또는 IPv6='::/'로 설정된 Amazon EC2 보안 그룹을 평가합니다. 보안 그룹에 그러한 대상 중 하나가 없는 경우 이 `NOT_APPLICABLE` 규칙이 반환됩니다.

식별자: VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

리소스 유형: AWS::EC2::SecurityGroup

트리거 유형: 구성 변경 및 주기적

AWS 리전: 아시아 태평양(멜버른) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

authorizedTcpPorts(선택 사항), 유형: 문자열

0.0.0.0/0 또는 ::/0으로 열 수 있도록 승인된 TCP 포트를 쉼표로 구분한 목록입니다. 범위는 대시로 정의됩니다(예: "443,1020-1025").

authorizedUdpPorts(선택 사항), 유형: 문자열

0.0.0.0/0 또는 ::/0으로 열 수 있도록 승인된 UDP 포트를 쉼표로 구분한 목록입니다. 범위는 대시로 정의됩니다(예: "500,1020-1025").

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

vpc-sg-port-restriction-check

보안 그룹이 수신 트래픽을 0.0.0.0/0 또는 ::/0에서 명시적으로 제한된 포트로 제한하는지 확인합니다. 보안 그룹이 TCP/UDP 포트 22/3389를 통해 또는 파라미터에 지정된 대로 0.0.0.0/0 또는 ::/0의 수신 트래픽을 허용하는 경우 규칙은 NON_COMPLIANT입니다.

식별자: VPC_SG_PORT_RESTRICTION_CHECK

리소스 유형: AWS::EC2::SecurityGroup

트리거 유형: 주기적

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(말레이시아), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

restrictPorts(선택 사항), 유형: CSV

전체 IP 범위에서 들어오는 트래픽에 대해 열면 안 되는 포트의 쉼표로 구분된 목록 유효한 포트 번호의 범위는 0~65535입니다. 지정되지 않은 경우 규칙은 기본적으로 22 및 3389를 확인합니다.

protocolType(선택 사항), 유형: 문자열

확인할 규칙의 전송 프로토콜 유형입니다. 유효한 값에는 'TCP', 'UDP' 및 'ALL'(대/소문자를 구분하지 않음)이 포함됩니다. 'ALL'로 설정하면 규칙은 'TCP', 'UDP' 또는 'ALL'(-1) 프로토콜을 사용하는 규칙을 확인합니다. 기본값은 'ALL'입니다.

excludeExternalSecurityGroups(선택 사항), 유형: boolean

외부 보안 그룹의 평가를 제외하는 부울 플래그입니다. 'true'로 설정하면 규칙이 외부 보안 그룹을 평가에 포함하지 않습니다. 그렇지 않으면 값이 'false'로 설정된 경우 모든 보안 그룹이 평가됩니다. 기본값은 'true'입니다.

ipType(선택 사항), 유형: 문자열

확인할 규칙의 인터넷 프로토콜(IP) 버전입니다. 유효한 값에는 'IPv4', 'IPv6' 및 'ALL'(대소문자를 구분하지 않음)이 포함됩니다. 지정하지 않으면 규칙은 기본적으로 'ALL'을 확인합니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

vpc-vpn-2-tunnels-up

Site AWS Site-to-Site VPN에서 제공하는 두 가상 프라이빗 네트워크(VPN) 터널이 모두 UP 상태인지 확인합니다. 두 터널 중 하나 또는 두 터널 모두 작동 중지 상태이면 규칙은 NON_COMPLIANT입니다.

식별자: VPC_VPN_2_TUNNELS_UP

리소스 유형: AWS::EC2::VPNConnection

트리거 0유형: 구성 변경

AWS 리전: 중동(바레인), 중국(베이징), 아시아 태평양(오사카), 이스라엘(텔아비브), 중국(닝샤) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

wafv2-logging-enabled

AWS WAFv2 리전 및 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되었지만 로깅 대상이 파라미터 값과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

> **Note**
>
> Amazon Security Lake 예외
> 이 규칙은 AWS WAFV2 웹 ACLs에 대해 Security Lake로 수행된 로깅을 확인하지 않습니다.

식별자: WAFV2_LOGGING_ENABLED

리소스 유형: AWS::WAFv2::WebACL

트리거 유형: 주기적

AWS 리전: 아시아 태평양(태국), 멕시코(중부), 아시아 태평양(타이베이) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

KinesisFirehoseDeliveryStreamArns(선택 사항), 유형: CSV

쉼표로 구분된 Kinesis Firehose 전송 스트림 ARN 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

wafv2-rulegroup-logging-enabled

AWS WAFv2 규칙 그룹의 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

컨텍스트: AWS WAFV2 (웹 애플리케이션 방화벽 버전 2)를 사용하면 일반적인 웹 악용 및 취약성으로부터 웹 애플리케이션을 보호하는 AWS WAF 규칙을 생성할 수 있습니다. AWS WAF 규칙 그룹은 웹 ACL(액세스 제어 목록)과 연결하여 웹 애플리케이션 트래픽에 대해 원하는 동작을 정의할 수 있는 AWS WAF 규칙 모음입니다. 자세한 내용은 AWS WAF 개발자 가이드의 AWS WAF 규칙 및 규칙 그룹을 참조하세요.

AWS WAFV2 규칙 그룹에서 CloudWatch 보안 지표 수집을 구성하면 성공 또는 실패한 분산 서비스 거부(DDoS), SQL 삽입 및 교차 사이트 스크립팅(XSS) 공격과 같은 보안 지표를 모니터링할 수 있습니다. 수집된 보안 지표는 조사를 간소화하는 데 도움이 될 수 있습니다.

> **Note**
>
> AWS WAFV2 규칙 그룹에 확인할 AWS Config 관리 AWS WAF 형 규칙에 대한 규칙이 없는 경우 AWS Config 관리형 규칙은를 반환합니다`NOT_APPLICABLE`.

식별자: WAFV2_RULEGROUP_LOGGING_ENABLED

리소스 유형: AWS::WAFv2::RuleGroup

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

wafv2-rulegroup-not-empty

WAFv2 리전 규칙 그룹에 규칙이 포함되어 있는지 확인합니다. WAFv2 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: WAFV2_RULEGROUP_NOT_EMPTY

리소스 유형: AWS::WAFv2::RuleGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), 아시아 태평양(멜버른), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

wafv2-webacl-not-empty

WAFv2 리전 웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: WAFV2_WEBACL_NOT_EMPTY

리소스 유형: AWS::WAFv2::WebACL

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리), 유럽(스페인), 유럽(취리히) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

waf-classic-logging-enabled

AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.

식별자: WAF_CLASSIC_LOGGING_ENABLED

리소스 유형: AWS::WAF::WebACL

트리거 유형: 주기적

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

KinesisFirehoseDeliveryStreamArns(선택 사항), 유형: CSV

AWS WAF 로그에 대한 Amazon Kinesis 스트림 ARN의 쉼표로 구분된 목록입니다.

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

waf-global-rulegroup-not-empty

AWS WAF Classic 규칙 그룹에 규칙이 포함되어 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: WAF_GLOBAL_RULEGROUP_NOT_EMPTY

리소스 유형: AWS::WAF::RuleGroup

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

waf-global-rule-not-empty

AWS WAF 글로벌 규칙에 조건이 포함되어 있는지 확인합니다. WAF 글로벌 규칙 내에 조건이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: WAF_GLOBAL_RULE_NOT_EMPTY

리소스 유형: AWS::WAF::Rule

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

waf-global-webacl-not-empty

WAF 글로벌 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.

식별자: WAF_GLOBAL_WEBACL_NOT_EMPTY

리소스 유형: AWS::WAF::WebACL

트리거 0유형: 구성 변경

AWS 리전: 미국 동부(버지니아 북부) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

waf-regional-rulegroup-not-empty

WAF 리전 규칙 그룹에 규칙이 포함되어 있는지 확인합니다. WAF 리전 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: WAF_REGIONAL_RULEGROUP_NOT_EMPTY

리소스 유형: AWS::WAFRegional::RuleGroup

트리거 0유형: 구성 변경

AWS 리전: 중국(베이징), 아시아 태평양(태국), 아시아 태평양(자카르타), 중동(UAE), 아시아 태평양(하이데라바드), 아시아 태평양(오사카), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 이스라엘(텔아비브), 캐나다 서부(캘거리), 유럽(스페인), 중국(닝샤), 유럽(취리히) 리전을 AWS 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

waf-regional-rule-not-empty

WAF 리전 규칙에 조건이 포함되어 있는지 확인합니다. 리전 규칙에 하나 이상의 조건이 포함되어 있으면 이 규칙은 COMPLIANT이고 그렇지 않으면 NON_COMPLIANT입니다.

식별자: WAF_REGIONAL_RULE_NOT_EMPTY

리소스 유형: AWS::WAFRegional::Rule

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

waf-regional-webacl-not-empty

WAF 리전 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL 내에 WAF 규칙 또는 규칙 그룹이 없는 경우 규칙은 NON_COMPLIANT입니다.

식별자: WAF_REGIONAL_WEBACL_NOT_EMPTY

리소스 유형: AWS::WAFRegional::WebACL

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(태국), 아시아 태평양(말레이시아), AWS GovCloud(미국 동부), AWS GovCloud(미국 서부), 멕시코(중부), 캐나다 서부(캘거리) AWS 리전을 제외한 지원되는 모든 리전

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

workspaces-root-volume-encryption-enabled

Amazon WorkSpace 볼륨에 루트 볼륨 암호화 설정이 활성화로 설정되어 있는지 확인합니다. 루트 볼륨 암호화 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: WORKSPACES_ROOT_VOLUME_ENCRYPTION_ENABLED

리소스 유형: AWS::WorkSpaces::Workspace

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 아프리카(케이프타운), 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부), 중국(닝샤) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

workspaces-user-volume-encryption-enabled

Amazon WorkSpace 볼륨에 사용자 볼륨 암호화 설정이 활성화로 설정되어 있는지 확인합니다. 사용자 볼륨 암호화 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

식별자: WORKSPACES_USER_VOLUME_ENCRYPTION_ENABLED

리소스 유형: AWS::WorkSpaces::Workspace

트리거 0유형: 구성 변경

AWS 리전: 아시아 태평양(뭄바이), 아프리카(케이프타운), 유럽(아일랜드), 유럽(프랑크푸르트), 남아메리카(상파울루), 미국 동부(버지니아 북부), 아시아 태평양(서울), 유럽(런던), 아시아 태평양(도쿄), 미국 서부(오레곤), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 캐나다(중부), 중국(닝샤) 리전에서만 사용 가능

파라미터:

없음

AWS CloudFormation 템플릿

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙을 생성하려면 섹션을 참조하세요AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성.

평가 모드별 AWS Config 관리형 규칙 목록

AWS Config 는 현재 다음과 같은 관리형 규칙을 지원합니다. 이러한 규칙을 사용하기 전에 섹션을 참조하세요고려 사항.

사전 평가

사전 예방 규칙은 배포되지 않은 리소스에 대한 사전 평가 모드를 지원하는 규칙입니다. 이를 통해 리소스 속성 집합을 사용하여 리소스를 정의하는 경우 해당 리전의 계정에 있는 사전 예방 규칙 집합을 고려하여 AWS 리소스 속성 집합이 COMPLIANT인지 NON_COMPLIANT인지 평가할 수 있습니다. 자세한 내용은 평가 모드를 참조하세요.

> **Note**
> 사전 예방 규칙은 규정 미준수로 플래그가 지정된 리소스를 수정하거나 배포를 금지하지 않습니다.

사전 평가

- api-gw-xray-enabled

- autoscaling-group-elb-healthcheck-required
- ec2-instance-multiple-eni-check
- eip-attached
- elasticsearch-node-to-node-encryption-check
- lambda-function-settings-check
- lambda-inside-vpc
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-public-access-check
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- s3-bucket-logging-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled

탐지 평가

탐지 규칙은 이미 배포된 리소스에 대한 탐지 평가 모드를 지원하는 규칙입니다. 이를 통해 기존 리소스의 구성 설정을 평가할 수 있습니다.

> **Note**
> 현재 모든 AWS Config 규칙은 탐지 평가를 지원합니다.

탐지 평가

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged

- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-cache-ct-encryption-in-transit

- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged

- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged

- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description

- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan

- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch

- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions

- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-saml-provider-tagged
- acm-certificate-expiration-check
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged

- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged

- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled

- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable

- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited

- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description

- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created

- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty

- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

트리거 유형별 AWS Config 관리형 규칙 목록

AWS Config 는 현재 다음과 같은 관리형 규칙을 지원합니다. 이러한 규칙을 사용하기 전에 섹션을 참조하세요고려 사항.

구성 변경

변경 트리거 규칙은 구성 변경에 대한 응답으로가 AWS Config 평가하는 규칙입니다.

구성 변경

- acmpca-certificate-authority-tagged
- acm-certificate-rsa-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged

- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check

- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-settings-check
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururreviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check

- ec2-client-vpn-connection-log-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-filesystem-ct-encrypted
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-supported-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check

- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged

- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-saml-provider-tagged
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-no-policies-check
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged

- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled

- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance

- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-postgresql-logs-to-cloudwatch
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted

- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- route53-query-logging-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-using-cmk
- service-catalog-shared-within-organization
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged

- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

주기적

주기적 규칙은 사용자가 지정한 빈도로, 예를 들어 24시간마다 주기적으로 AWS Config 평가하는 규칙입니다.

주기적

- access-keys-rotated
- account-part-of-organizations

- acm-pca-root-ca-disabled
- alb-http-to-https-redirection-check
- api-gwv2-authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- cloudfront-s3-origin-non-existent-bucket
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-resources-protected-by-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-last-backup-recovery-point-created
- ec2-meets-restore-time-target
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ecr-private-image-scanning-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eks-cluster-logging-enabled
- eks-secrets-encrypted

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2-acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- event-data-store-cmk-encryption-enabled
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled

- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- acm-certificate-expiration-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- kinesis-firehose-delivery-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-automatic-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- multi-region-cloud-trail-enabled
- netfw-logging-enabled

- nlb-logging-enabled
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-mysql-instance-encrypted-in-transit
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-sqlserver-encrypted-in-transit
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-account-level-public-access-blocks-periodic
- s3-last-backup-recovery-point-created
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version

- sagemaker-notebook-no-direct-internet-access
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- waf-classic-logging-enabled

하이브리드

하이브리드 규칙은 구성 변경에 대응하여 정기적으로 AWS Config 평가하는 규칙입니다.

하이브리드

- acm-certificate-expiration-check

- cloudformation-stack-drift-detection-check
- ec2-instance-launched-with-allowed-ami
- incoming-ssh-disabled
- restricted-incoming-traffic
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

리전 가용성별 AWS Config 관리형 규칙 목록

AWS Config 는 현재 다음과 같은 관리형 규칙을 지원합니다. 이러한 규칙을 사용하기 전에 섹션을 참조하세요고려 사항.

US East (Ohio) Region

미국 동부(오하이오)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged

- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on

- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged

- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created

- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached

- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged

- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan

- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created

- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only

- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

미국 동부(버지니아 북부) 리전

미국 동부(버지니아 북부)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged

- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled

- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururreviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged

- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check

- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged

- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version

- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit

- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest

- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-saml-provider-tagged
- acm-certificate-expiration-check
- iam-server-certificate-tagged
- iam-user-group-membership-check
- iam-user-mfa-enabled

- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged

- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled

- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled

- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target

- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access

- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled

- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled

- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed

- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

US West (N. California) Region

미국 서부(캘리포니아 북부)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage

- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled

- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check

- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check

- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled

- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted

- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured

- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version

- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled

- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled

- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled

- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled

- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access

- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault

- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access

- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

US West (Oregon) Region

미국 서부(오리건)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled

- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists

- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled

- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled

- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check

- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged

- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created

- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled

- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged

- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged

- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs

- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled

- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled

- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged

- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version

- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled

- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

아프리카(케이프타운) 리전

아프리카(케이프타운)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage

- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging

- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging

- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged

- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged

- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check

- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description

- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check

- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled

- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled

- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check

- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access

- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check

- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Asia Pacific (Hong Kong) Region

아시아 태평양(홍콩)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled

- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged

- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted

- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled

- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled

- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault

- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user

- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check

- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions

- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited

- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled

- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

아시아 태평양(하이데라바드) 리전

아시아 태평양(하이데라바드)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled

- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit

- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target

- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target

- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted

- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access

- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled

- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited

- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms

- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Asia Pacific (Jakarta) Region

아시아 태평양(자카르타)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding

- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-report-group-encrypted-at-rest
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check

- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled

- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled

- eks-cluster-log-enabled
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest

- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled

- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc

- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault

- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

아시아 태평양(말레이시아) 리전

아시아 태평양(말레이시아)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled

- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw

- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Asia Pacific (Melbourne) Region

아시아 태평양(멜버른)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled

- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan

- ec2-security-group-attached-to-eni
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan

- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check

- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check

- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty

- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch

- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged

- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Asia Pacific (Mumbai) Region

아시아 태평양(뭄바이)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description

- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description

- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template

- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging

- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged

- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic

- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory

- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created

- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled

- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled

- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled

- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch

- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled

- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Asia Pacific (Osaka) Region

아시아 태평양(오사카)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-internal-scheme-check
- alb-listener-tagged
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled

- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged

- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-tagged
- dynamodb-autoscaling-enabled

- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created

- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled

- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-cross-zone-load-balancing-enabled
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs

- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets

- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az

- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check

- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Asia Pacific (Seoul) Region

아시아 태평양(서울)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged

- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on

- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled

- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted

- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access

- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized

- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged

- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check

- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets

- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check

- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault

- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

아시아 태평양(싱가포르) 리전

아시아 태평양(싱가포르)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled

- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description

- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration

- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update

- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public

- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all

- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check

- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description

- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged

- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized

- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged

- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check

- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled

- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled

- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version

- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged

- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

아시아 태평양(시드니) 리전

아시아 태평양(시드니)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description

- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest

- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled

- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled

- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check

- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault

- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged

- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check

- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest

- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled

- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled

- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check

- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance

- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited

- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged

- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled

- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty

- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

아시아 태평양(타이베이) 리전

아시아 태평양(타이베이)

- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- cloudformation-stack-drift-detection-check
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled

- dynamodb-table-encryption-enabled
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-stopped-instance
- eip-attached
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- encrypted-volumes
- incoming-ssh-disabled
- instances-in-vpc
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

아시아 태평양(태국) 리전

아시아 태평양(태국)

- account-part-of-organizations

- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan

- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled

- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

아시아 태평양(도쿄) 리전

아시아 태평양(도쿄)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged

- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding

- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created

- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check

- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged

- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging

- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default

- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic

- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory

- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged

- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled

- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged

- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check

- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled

- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled

- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled

- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured

- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled

- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

캐나다(중부) 리전

캐나다(중부)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description

- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged

- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest

- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging

- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all

- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni

- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check

- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description

- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check

- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only

- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged

- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public

- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty

- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

캐나다 서부(캘거리) 리전

캐나다 서부(캘거리)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- batch-scheduling-policy-tagged
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cognito-user-pool-tagged
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-prefix-list-tagged
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ecr-repository-tagged
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled

- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nlb-internal-scheme-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted

- rds-storage-encrypted
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-tagged
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

중국(베이징) 리전

중국(베이징)

- access-keys-rotated
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled

- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- athena-workgroup-logging-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-s3-origin-non-existent-bucket
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging

- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance

- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled

- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode

- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public

- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

중국(닝샤) 리전

중국(닝샤)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check

- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- athena-workgroup-logging-enabled
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check

- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled

- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest

- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- glue-job-logging-enabled
- glue-spark-job-supported-version
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check

- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted

- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled

- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access

- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Europe (Frankfurt) Region

유럽(프랑크푸르트)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage

- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled

- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged

- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted

- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured

- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan

- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged

- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version

- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit

- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled

- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc

- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged
- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited

- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check

- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit

- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks

- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count

- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault

- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Europe (Ireland) Region

유럽(아일랜드)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access

- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted

- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled

- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan

- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-enabled
- ivs-channel-playback-authorization-enabled
- ivs-channel-tagged

- ivs-playback-key-pair-tagged
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw

- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled

- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch

- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization

- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Europe (London) Region

유럽(런던)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check

- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged

- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created

- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check

- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged

- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-profile-creation
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging

- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default

- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance

- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled

- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled

- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted

- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited

- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description

- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled

- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

Europe (Milan) Region

유럽(밀라노)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description

- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-workgroup-description

- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update

- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled

- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached

- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled

- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted

- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled

- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted

- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp

- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled

- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled

- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only

- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed

- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Europe (Paris) Region

유럽(파리)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged

- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged

- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-access
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging

- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check

- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled

- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip

- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled

- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault

- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az

- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- glb-listener-tagged
- global-endpoint-event-replication-enabled

- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check

- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled

- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled

- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl

- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only

- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan

- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

유럽(스페인) 리전

유럽(스페인)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check

- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan

- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled

- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted

- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl

- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled

- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled

- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Europe (Stockholm) Region

유럽(스톡홀름)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged

- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target

- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check

- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check

- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled

- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled

- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled

- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check

- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs

- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty

- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled

- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3express-dir-bucket-lifecycle-rules-check
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

유럽(취리히) 리전

유럽(취리히)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description

- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created

- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest

- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled

- iam-password-policy
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty

- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted

- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encrypted-in-transit
- redshift-serverless-workgroup-no-public-access
- redshift-serverless-workgroup-routes-within-vpc
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic

- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Israel (Tel Aviv) Region

이스라엘(텔아비브)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description

- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-logging
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached

- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-prefix-list-tagged
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-mount-target-public-accessible
- eip-attached
- eks-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted

- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled

- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- macie-auto-sensitive-data-discovery-check
- mariadb-publish-logs-to-cloudwatch-logs
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-multi-az-support

- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled

- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- subnet-auto-assign-public-ip-disabled
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

멕시코(중부) 리전

멕시코(중부)

- account-part-of-organizations

- acm-certificate-expiration-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launch-config-public-ip-disabled
- cloudformation-stack-drift-detection-check
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms

- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-encryption-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

Middle East (Bahrain) Region

중동(바레인)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted

- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged

- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check

- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged

- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan

- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan

- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Middle East (UAE) Region

중동(UAE)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- codebuild-report-group-encrypted-at-rest
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created

- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged

- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eks-cluster-log-enabled
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan

- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-enabled
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited

- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mariadb-publish-logs-to-cloudwatch-logs
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-access
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled

- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

South America (São Paulo) Region

남아메리카(상파울루)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-deletion-enabled
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-enabled
- amplify-branch-tagged

- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-not-empty
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-to-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-storage
- appconfig-hosted-configuration-version-description
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-forwarding
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-defaults-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged

- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-cache-ct-encryption-in-transit
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-rest
- athena-workgroup-enforce-workgroup-configuration
- athena-workgroup-engine-version-auto-upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-cluster-audit-logging
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-enabled
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-deployment-group-auto-rollback-enabled
- codedeploy-deployment-group-outdated-instances-update
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-access-check
- cognito-user-pool-advanced-security-enabled
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- datasync-task-data-verification-enabled
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-tagged
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created

- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-capacity-reservation-tagged
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-all
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-플릿 태그 지정
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-imdsv2-check
- ec2-launch-template-public-ip-disabled
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-meets-restore-time-target
- ec2-network-insights-access-scope-analysis-tagged
- ec2-network-insights-access-scope-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-transit-gateway-multicast-domain-tagged
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check

- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- emr-security-configuration-encryption-rest
- emr-security-configuration-encryption-transit
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fis-experiment-template-log-configuration-exists
- fis-experiment-template-tagged
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-ontap-deployment-type-check
- fsx-openzfs-copy-tags-enabled
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- fsx-windows-deployment-type-check
- glb-listener-tagged
- global-endpoint-event-replication-enabled
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-enabled
- guardduty-eks-protection-audit-enabled
- guardduty-eks-protection-runtime-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-external-access-analyzer-enabled
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged

- iot-authorizer-token-signing-enabled
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- kms-key-policy-no-public-access
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie-auto-sensitive-data-discovery-check
- macie-status-check
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-active-broker-ldap-authentication
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-broker-general-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-disabled
- msk-connect-connector-logging-enabled
- msk-enhanced-monitoring-enabled

- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-cross-zone-load-balancing-enabled
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest

- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-logging-enabled
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit

- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-parameter-group-tagged
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-no-public-access
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-app-image-config-tagged
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- sns-topic-no-public-access
- sqs-queue-no-public-access
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

AWS GovCloud(미국 동부) 리전

AWS GovCloud(미국 동부)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-mysql-cluster-audit-logging

- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check

- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default

- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check

- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip

- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-spark-job-supported-version
- guardduty-eks-protection-audit-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled

- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-cloudwatch-audit-logging-enabled
- msk-cluster-public-access-disabled
- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-logging-enabled
- no-unrestricted-route-to-igw

- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled

- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

AWS GovCloud(미국 서부) 리전

AWS GovCloud(미국 서부)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id

- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-point-created
- aurora-mysql-cluster-audit-logging
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- s3-bucket-level-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-at-rest
- cognito-identity-pool-unauth-access-check
- connect-instance-logging-enabled
- cw-loggroup-retention-period-check
- datasync-task-logging-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-enabled
- dms-neptune-iam-authorization-enabled
- dms-redis-tls-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-enis-source-destination-check-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ec2-client-vpn-connection-log-enabled
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecr-repository-cmk-encryption-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- 전송 중 elbv2-listener-encryption-in-transit
- elbv2-predefined-security-policy-ssl-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- event-data-store-cmk-encryption-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-ontap-deployment-type-check
- fsx-openzfs-deployment-type-check
- fsx-resources-protected-by-backup-plan
- fsx-windows-deployment-type-check
- glue-job-logging-enabled
- glue-ml-transform-encrypted-at-rest
- glue-spark-job-supported-version
- guardduty-eks-protection-audit-enabled
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- acm-certificate-expiration-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ec2-scan-enabled
- inspector-lambda-code-scan-enabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream-encrypted
- kinesis-stream-backup-retention-check
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-logs
- mfa-enabled-for-iam-console-access
- mq-cloudwatch-audit-logging-enabled
- msk-cluster-public-access-disabled

- msk-unrestricted-access-check
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- netfw-subnet-change-protection-enabled
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-data-node-fault-tolerance
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-to-cloudwatch
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-instance-subnet-igw-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-mariadb-instance-encrypted-in-transit
- rds-multi-az-support
- rds-mysql-instance-encrypted-in-transit
- rds-postgresql-logs-to-cloudwatch
- rds-postgres-instance-encrypted-in-transit

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-transit
- rds-sql-server-logs-to-cloudwatch
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-enabled
- redshift-cluster-public-access-check
- redshift-cluster-subnet-group-multi-az
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-serverless-default-admin-check
- redshift-serverless-default-db-name-check
- redshift-serverless-namespace-cmk-encryption
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-cross-region-replication-enabled
- s3-bucket-default-lock-enabled

- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-platform-version
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-organization
- service-vpc-endpoint-enabled

- sns-encrypted-kms
- ssm-automation-block-public-sharing
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-check
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- workspaces-root-volume-encryption-enabled
- workspaces-user-volume-encryption-enabled

AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성

> **Important**
>
> AWS Config 관리형 규칙을 생성하려면 먼저 AWS Config 구성 레코더를 생성하고 시작해야 합니다 AWS CloudFormation. 자세한 내용은 구성 레코더 관리를 참조하십시오.

지원되는 AWS Config 관리형 규칙의 경우 AWS CloudFormation 템플릿을 사용하여 계정에 대한 규칙을 생성하거나 기존 AWS CloudFormation 스택을 업데이트할 수 있습니다. 스택이란 하나의 단위

로 프로비저닝 및 업데이트하는 관련 리소스의 모음입니다. 템플릿을 사용하여 스택을 시작하면 AWS Config 관리형 규칙이 생성됩니다. 템플릿은 규칙만 생성하고 추가 AWS 리소스를 생성하지 않습니다.

> **Note**
>
> AWS Config 관리형 규칙이 업데이트되면 최신 변경 사항에 맞게 템플릿이 업데이트됩니다. 규칙을 위해 특정 버전의 템플릿을 저장하려면 해당 템플릿을 다운로드한 다음 이를 S3 버킷에 업로드합니다.

AWS CloudFormation 템플릿 작업에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 시작하기 AWS CloudFormation를 참조하세요.

AWS Config 관리형 규칙의 AWS CloudFormation 스택을 시작하려면

1. CloudFormation 콘솔로 이동하여 새 스택을 생성합니다.
2. 템플릿 지정의 경우 다음을 수행합니다.
   - 템플릿을 다운로드한 경우, 템플릿 파일 업로드를 선택한 다음 파일 선택을 선택하여 템플릿을 업로드합니다.
   - Amazon S3 URL을 선택하고 템플릿 URL `http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/THE_RULE_IDENTIFIER.template`을 입력할 수도 있습니다.

   > **Note**
   >
   > 규칙 식별자는 ALL_CAPS_WITH_UNDERSCORES로 작성해야 합니다. 예를 들어, cloudwatch-log-group-encrypted 대신 CLOUDWATCH_LOG_GROUP_ENCRYPTED를 사용합니다.
   > 일부 규칙의 경우 규칙 식별자가 규칙 이름과 다릅니다. 규칙 식별자를 사용해야 합니다. 예를 들어, restricted-ssh의 규칙 식별자는 INCOMING_SSH_DISABLED입니다.

3. Next(다음)를 선택합니다.
4. 스택 세부 정보 지정에 스택 이름을 입력하고 AWS Config 규칙의 파라미터 값을 입력합니다. 예를 들어, `DESIRED_INSTANCE_TYPE` 관리형 규칙 템플릿을 사용 중인 경우 "m4.large" 등의 인스턴스 유형을 지정할 수 있습니다.
5. Next(다음)를 선택합니다.

6. [Options]에서 태그를 만들거나 다른 고급 옵션을 구성할 수 있습니다. 이는 필수는 아닙니다.
7. Next(다음)를 선택합니다.
8. 검토에서 템플릿, 파라미터 및 기타 옵션이 올바른지 확인합니다.
9. 생성(Create)을 선택합니다. 스택이 몇 분 내에 생성됩니다. AWS Config 콘솔에서 생성된 규칙을 볼 수 있습니다.

템플릿을 사용하여 AWS Config 관리형 규칙에 대한 단일 스택을 생성하거나 계정의 기존 스택을 업데이트할 수 있습니다. 스택을 삭제하면 해당 스택에서 생성된 관리형 규칙도 삭제됩니다. 자세한 내용을 알아보려면 AWS CloudFormation 사용 설명서의 스택 작업을 참조하세요.

AWS Config 사용자 지정 규칙

AWS Config 사용자 지정 규칙은 처음부터 생성하는 규칙입니다. 사용자 AWS Config 지정 규칙을 생성하는 방법에는 Lambda 함수(AWS Lambda 개발자 안내서)와 policy-as-code 언어인 Guard(Guard GitHub Repository)의 두 가지가 있습니다.

AWS Config Lambda로 생성된 사용자 지정 규칙을 AWS Config 사용자 지정 Lambda 규칙이라고 하고 Guard로 생성된 AWS Config 사용자 지정 규칙을 사용자 AWS Config 지정 정책 규칙이라고 합니다.

사용자 지정 규칙을 사용하기 전에 섹션을 참조하세요고려 사항.

AWS Config 사용자 지정 정책 규칙

Guard를 사용하여 작성된 규칙은 AWS Config 콘솔에서 생성하거나 AWS Config 규칙 APIs를 사용하여 생성할 수 있습니다. AWS Config 사용자 지정 정책 규칙을 사용하면 Java 또는 Python을 사용하여 AWS Config 사용자 지정 규칙을 관리하기 위한 Lambda 함수를 개발할 필요 없이 사용자 지정 규칙을 생성할 수 있습니다. AWS Config 사용자 지정 정책 규칙은 구성 변경에 의해 시작됩니다. Guard에 자세한 내용은 GitHub에서 Guard GitHub 리포지토리를 참조하세요.

AWS Config 사용자 지정 Lambda 규칙

사용자 지정 Lambda 규칙은 Java 또는 Python을 사용하여 AWS Config 사용자 지정 규칙에 대한 Lambda 함수를 생성하는 옵션을 제공합니다. Lambda 함수는 사용자가 업로드하는 사용자 지정 코드 AWS Lambda이며 이벤트 소스에서 게시하는 이벤트에 의해 호출됩니다. Lambda 함수가 AWS Config 규칙 AWS Config 과 연결된 경우는 규칙이 시작될 때 이를 호출합니다. 그런 다음 Lambda 함수는에서 전송한 구성 정보를 평가하고 평가 결과를 AWS Config반환합니다. Lambda 함수에 대한 자세한 내용은 AWS Lambda 개발자 안내서의 함수 및 이벤트 소스를 참조하세요.

AWS Config 사용자 지정 규칙의 형식 차이

다음 표에는 ConfigurationItem 데이터 유형 및 AWS Config 사용자 지정 규칙에 대한 필드의 형식 차이가 표시됩니다.

ConfigurationItem	AWS Config 사용자 지정 규칙
`version`	`configurationItemVersion`
`accountId`	`awsAccountId`
`arn`	`ARN`
`configurationItemMD5Hash`	`configurationStateMd5Hash`

주제

- AWS Config 사용자 지정 정책 규칙 생성
- AWS Config 사용자 지정 Lambda 규칙 생성
- AWS Config 사용자 지정 Lambda 규칙을 사용하여 삭제된 리소스 관리

AWS Config 사용자 지정 정책 규칙 생성

AWS Management Console AWS CLI또는 AWS Config API에서 AWS Config 사용자 지정 정책 규칙을 생성할 수 있습니다.

AWS Config 사용자 지정 정책 규칙 추가

Using the console

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Management Console 메뉴에서 리전 선택기가 AWS Config 규칙을 지원하는 리전으로 AWS 설정되어 있는지 확인합니다. 지원되는 리전의 목록은 Amazon Web Services 일반 참조의 AWS Config 리전 및 엔드포인트를 참조하세요.
3. 왼쪽 탐색 창에서 규칙을 선택합니다.
4. 규칙 페이지에서 규칙 추가를 선택합니다.

5. 규칙 유형 지정 페이지에서 Guard를 사용하여 사용자 지정 규칙 생성을 선택합니다.
6. 규칙 구성 페이지에서 다음 단계를 완료하여 규칙을 생성합니다.

   a. 규칙 이름에 규칙의 고유 이름을 입력합니다.
   b. 설명에 규칙에 대한 설명을 입력합니다.
   c. Guard 런타임 버전에서 AWS Config 사용자 지정 정책 규칙의 런타임 시스템을 선택합니다.
   d. 규칙 내용의 경우 규칙의 Guard 사용자 지정 정책으로 채울 수 있습니다.
   e. 평가 모드에서 리소스 생성 및 관리 프로세스에서 리소스를 평가 AWS Config 하려는 시기를 선택합니다. 규칙에 따라는 리소스가 프로비저닝되기 전, 리소스가 프로비저닝된 후 또는 둘 다 수행하기 전에 리소스 구성을 평가할 AWS Config 수 있습니다.

      i. 리소스를 배포하기 전에 리소스의 구성 설정에 대한 평가를 실행하려면 사전 평가 켜기를 선택합니다.

         사전 평가를 활성화한 후에는 StartResourceEvaluation API 및 GetResourceEvaluationSummary API를 사용하여 이러한 명령에 지정한 리소스가 해당 계정의 해당 리전 사전 예방 규칙에 따라 NON_COMPLIANT 플래그가 지정되는지 확인할 수 있습니다.

         이 명령 사용에 대한 자세한 내용은 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 사전 평가를 지원하는 관리형 규칙 목록은 평가 모드별 AWS Config 관리형 규칙 목록을 참조하세요.

      ii. 기존 리소스의 구성 설정을 평가하려면 탐지 평가 켜기를 선택합니다.

         탐지 평가를 위해 AWS Config 사용자 지정 정책 규칙은 구성 변경에 의해 시작됩니다. 이 옵션은 미리 선택되어 있습니다.

         - 리소스 - 지정된 리소스 유형 또는 유형 및 식별자와 일치하는 리소스가 생성, 변경 또는 삭제되는 경우.
         - 태그 - 지정된 태그가 있는 리소스가 생성, 변경 또는 삭제되는 경우.
         - 모든 변경 사항 -에 의해 기록된 리소스 AWS Config 가 생성, 변경 또는 삭제되는 경우.

         AWS Config 는 규칙의 범위와 일치하는 리소스에 대한 변경을 감지하면 평가를 실행합니다. 범위를 사용하여 평가를 시작하는 리소스를 제한할 수 있습니다. 그렇지 않으면 사후 프로비저닝된 리소스가 변경될 때 평가가 시작됩니다.

f. 규칙에 파라미터가 포함된 경우 파라미터에서 제공된 키의 값을 사용자 지정할 수 있습니다. 파라미터는 리소스가 규칙을 준수한다고 간주되기 위해 준수해야 하는 속성입니다.

7. 검토 및 생성 페이지에서 모든 선택 사항을 검토한 후 AWS 계정에 규칙을 추가합니다.
8. 규칙 검토를 마치면 규칙 추가를 선택합니다.

Using the AWS CLI

put-config-rule 명령을 사용합니다.

Owner 필드는 CUSTOM_POLICY여야 합니다. AWS Config 사용자 지정 정책 규칙에는 다음과 같은 추가 필드가 필요합니다.

- Runtime: AWS Config 사용자 지정 정책 규칙의 런타임 시스템입니다.
- PolicyText: AWS Config 사용자 지정 정책 규칙에 대한 논리가 포함된 정책 정의입니다.
- EnableDebugLogDelivery: AWS Config 사용자 지정 정책 규칙에 대한 디버그 로깅을 활성화하기 위한 부울 표현식입니다. 기본값은 false입니다.

Using the API Reference

PutConfigRule 작업을 사용합니다.

Owner 필드는 CUSTOM_POLICY여야 합니다. AWS Config 사용자 지정 정책 규칙에는 다음과 같은 추가 필드가 필요합니다.

- Runtime: AWS Config 사용자 지정 정책 규칙의 런타임 시스템입니다.
- PolicyText: AWS Config 사용자 지정 정책 규칙에 대한 논리가 포함된 정책 정의입니다.
- EnableDebugLogDelivery: AWS Config 사용자 지정 정책 규칙에 대한 디버그 로깅을 활성화하기 위한 부울 표현식입니다. 기본값은 false입니다.

AWS Config 사용자 지정 정책 규칙에 대한 규칙 콘텐츠 작성

AWS Config 사용자 지정 정책 규칙을 사용하면 AWS CloudFormation Guard의 도메인별 언어(DSL)를 사용하여 리소스 구성을 평가할 수 있습니다. 이 주제에서는 사용자 지정 정책 규칙을 작성하기 위한 패턴과 모범 사례를 제공합니다.

Guard로 규칙을 작성하는 방법에 대한 자세한 내용은 Guard 사용 설명서의 Guard 규칙 작성 및 AWS CloudFormation Guard GitHub 리포지토리의 Guard 2.0 작업 모드를 참조하세요. AWS CloudFormation GitHub

기본 규칙 구조

다음 기본 형식을 사용하여 규칙을 생성합니다.

```
# Basic rule format
rule <rule_name> when
    resourceType == "<AWS::Service::Resource>" {
    # Evaluation clauses
}

# Example with filtering
let resources_of_type = Resources.*[ Type == 'AWS::Service::Resource' ]
rule check_resources when %resources_of_type !empty {
    %resources_of_type.configuration.property == expected_value
}
```

핵심 구성 요소

구성

리소스 구성에 대한 내용을 포함합니다.

supplementaryConfiguration

리소스 구성에 대한 추가 내용을 포함합니다. 구성 필드에 대해 반환된 정보를 보완하기 위해 특정 리소스 유형에 대해이 필드를 AWS Config 반환합니다.

resourceType

AWS 평가 중인 리소스 유형입니다.

resourceId

리소스의 ID입니다(예: `sg-xxxxxx`).

accountId

리소스와 연결된 12자리 AWS 계정 ID입니다.

일반적인 패턴

Status checks

```
let allowed_status = ['ACTIVE', 'RUNNING']
rule check_resource_status when
    resourceType == "AWS::Service::Resource" {
    configuration.status IN %allowed_status
}
```

Required properties

```
rule check_required_properties when
    resourceType == "AWS::Service::Resource" {
    configuration.propertyName exists
    configuration.propertyName is_string  # or is_list, is_struct
}
```

Query blocks

```
configuration.Properties {
    property1 exists
    property2 is_string
    property3 IN [allowed_value1, allowed_value2]
}
```

Conditional evaluation

```
when configuration.feature_enabled == true {
    configuration.feature_settings exists
    configuration.feature_settings is_struct
}
```

Custom messages

```
rule check_compliance when
    resourceType == "AWS::Service::Resource" {
    configuration.property == expected_value <<Custom error message explaining the
 requirement>>
}}
```

고급 기능

Range checks

```
rule check_numeric_limits {
    # Inclusive range (lower_limit <= value <= upper_limit)
    configuration.value IN r[minimum_value, maximum_value]

    # Exclusive range (lower_limit < value < upper_limit)
    configuration.value IN r(exclusive_min, exclusive_max)

    # Left inclusive, right exclusive (lower_limit <= value < upper_limit)
    configuration.value IN r[minimum_value, exclusive_max)

    # Left exclusive, right inclusive (lower_limit < value <= upper_limit)
    configuration.value IN r(exclusive_min, maximum_value]
}
```

Combining conditions

```
# AND conditions (implicit through new lines)
condition_1
condition_2

# OR conditions (explicit)
condition_3 OR
condition_4
```

Chaining rules

```
rule check_prerequisites {
    configuration.required_setting exists
}

rule check_details when check_prerequisites {
    configuration.required_setting == expected_value
}
```

모범 사례

- 가독성을 높이기 위해 `let` 문과 함께 변수를 사용합니다.

- 명명된 규칙 블록을 사용하여 관련 검사를 그룹화합니다.
- 설명이 포함된 설명을 포함합니다.
- 적절한 연산자(`exists`, `is_string`, `is_list`)를 사용합니다.
- 대/소문자를 구분하지 않는 일치와 함께 정규식 패턴을 사용합니다.

예: dynamodb-pitr-enabled

다음 예제에서는 AWS Config 관리형 규칙의 AWS Config 사용자 지정 정책 규칙 버전에 대한 정책 정의를 보여줍니다dynamodb-pitr-enabled. 이 규칙은 DynamoDB 테이블에 Point-in-Time으로 복구가 활성화되어 있는지 확인합니다.

```
# Check if DynamoDB tables have Point-in-Time Recovery enabled
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
    let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription.pointIn
    %pitr == "ENABLED" <<DynamoDB tables must have Point-in-Time Recovery enabled>>
}
```

AWS Config 사용자 지정 Lambda 규칙 생성

사용자 지정 규칙을 개발하고 AWS Lambda 함수 AWS Config 를 사용하여에 추가할 수 있습니다.

각 사용자 지정 규칙을 Lambda 함수와 연결합니다.이 함수에는 AWS 리소스가 규칙을 준수하는지 여부를 평가하는 로직이 포함되어 있습니다. 이 함수를 규칙에 연결하면, 이 규칙이 구성 변경에 대한 응답으로 또는 주기적으로 함수를 호출합니다. 그런 다음 함수는 리소스가 규칙을 준수하는지 여부를 평가하고 평가 결과를 로 보냅니다 AWS Config.

AWS 규칙 개발 키트(RDK)

AWS 규칙 개발 키트(RDK)는 직관적이고 생산적인 “Compliance-as-Code” 워크플로를 지원하도록 설계되었습니다. 사용자 지정 Lambda 함수가 지원하는 배포 AWS Config 규칙과 관련된 차별화되지 않은 과도한 작업을 대부분 추상화하고 간소화된 develop-deploy-monitor 반복 프로세스를 제공합니다.

step-by-step 지침은 AWS 규칙 개발 키트(RDK) 설명서를 참조하세요.

AWS Config 규칙에 대한 AWS Lambda 함수 예제(Node.js)

AWS Lambda 는 AWS 서비스에서 게시한 이벤트에 대한 응답으로 함수를 실행합니다. AWS Config 사용자 지정 Lambda 규칙의 함수는에서 게시한 이벤트를 수신한 다음 AWS Config이벤트에서 수신한 데이터와 AWS Config API에서 검색한 데이터를 사용하여 규칙의 규정 준수를 평가합니다. 구성 규칙의 함수 작업은 구성 변경으로 트리거된 평가를 수행하는지 주기적으로 트리거된 평가를 수행하는지에 따라 다릅니다.

AWS Lambda 함수 내의 일반적인 패턴에 대한 자세한 내용은 AWS Lambda 개발자 안내서의 프로그래밍 모델을 참조하세요.

Example Function for Evaluations Triggered by Configuration Changes

AWS Config 는 사용자 지정 규칙의 범위 내에 있는 리소스에 대한 구성 변경을 감지하면 다음 예제와 같은 함수를 호출합니다.

AWS Config 콘솔을 사용하여이 예제와 같은 함수와 연결된 규칙을 생성하는 경우 트리거 유형으로 구성 변경을 선택합니다. AWS Config API 또는를 사용하여 규칙을 AWS CLI 생성하는 경우 `MessageType` 속성을 `ConfigurationItemChangeNotification` 및 로 설정합니다`OversizedConfigurationItemChangeNotification`. 이러한 설정을 사용하면가 리소스 변경으로 인해 구성 항목 또는 크기 초과 구성 항목을 AWS Config 생성할 때마다 규칙을 트리거할 수 있습니다.

이 예제에서는 리소스를 평가하고 인스턴스가 리소스 유형 `AWS::EC2::Instance`와 일치하는지 확인합니다. AWS Config 가 구성 항목 또는 크기를 초과한 구성 항목 알림을 생성하면 규칙이 트리거됩니다.

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});
```

```
// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory
 API.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
    );

}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
```

```
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem)
 => {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
}

// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}

// In this example, the resource is compliant if it is an instance and its type
 matches the type specified as the desired type.
```

```
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration,
 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is
 not compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
```

```
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
};
```

함수 작업

함수는 실행 시 다음 작업을 수행합니다.

1. 함수는가 `event` 객체를 `handler` 함수에 AWS Lambda 전달할 때 실행됩니다. 이 예제에서 함수는 호출자에게 정보를 반환하는 데 사용하는 선택적 `callback` 파라미터를 수락합니다. AWS Lambda 또한 함수가 실행되는 동안 사용할 수 있는 정보와 메서드가 포함된 `context` 객체를 전달합니다. 참고로, 최신 버전의 Lambda에서는 컨텍스트가 더 이상 사용되지 않습니다.
2. 함수는 이벤트의 `messageType`이 구성 항목인지 크기를 초과한 구성 항목인지 확인한 다음, 해당 구성 항목을 반환합니다.
3. 핸들러는 `isApplicable` 함수를 호출하여 리소스가 삭제되었는지 여부를 확인합니다.

> **Note**
>
> 삭제된 리소스에 대해 보고하는 규칙은 불필요한 규칙 평가를 피하기 위해 `NOT_APPLICABLE` 평가 결과를 반환해야 합니다.

4. 핸들러는 `evaluateChangeNotificationCompliance` 함수를 호출하고 이벤트에 AWS Config 게시된 `configurationItem` 및 `ruleParameters` 객체를 전달합니다.

함수는 먼저 리소스가 EC2 인스턴스인지 여부를 평가합니다. 리소스가 EC2 인스턴스가 아닌 경우, 함수는 준수 값 `NOT_APPLICABLE`을 반환합니다.

그런 다음 함수는 구성 항목의 `instanceType` 속성이 `desiredInstanceType` 파라미터 값과 같은지 여부를 평가합니다. 값이 같으면 함수는 `COMPLIANT`를 반환합니다. 값이 같지 않으면 함수는 `NON_COMPLIANT`를 반환합니다.

5. 핸들러는 `putEvaluationsRequest` 객체를 초기화하여 평가 결과를 AWS Config 로 전송할 준비를 합니다. 이 객체에는 준수 결과를 식별하는 `Evaluations` 파라미터, 리소스 유형, 평가된 리소스의 ID가 포함되어 있습니다. `putEvaluationsRequest` 객체에는 규칙과 이벤트를 식별하는 이벤트의 결과 토큰도 포함됩니다 AWS Config.
6. 핸들러는 객체를 `config` 클라이언트의 `putEvaluations` 메서드에 전달 AWS Config 하여 평가 결과를에 전송합니다.

Example Function for Periodic Evaluations

AWS Config 는 정기 평가를 위해 다음 예제와 같은 함수를 호출합니다. 주기적 평가는 사용자가 AWS Config에서 규칙을 정의할 때 지정한 간격으로 발생합니다.

AWS Config 콘솔을 사용하여이 예제와 같은 함수와 연결된 규칙을 생성하는 경우 트리거 유형으로 주기적을 선택합니다. AWS Config API 또는를 사용하여 규칙을 AWS CLI 생성하는 경우 `MessageType` 속성을 로 설정합니다`ScheduledNotification`.

이 예제에서는 지정한 총 리소스 수가 지정한 최대치를 초과하는지 확인합니다.

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON
 objects passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;
```

```
   if (isScheduledNotification(invokingEvent) &&
hasValidRuleParameters(ruleParameters, callback)) {
       await countResourceTypes(ruleParameters.applicableResourceType, "",
numberOfResources, async function (err, count) {
           if (err === null) {
               var putEvaluationsRequest;
               const compliance = evaluateCompliance(ruleParameters.maxCount,
count);
               var annotation = '';
               if (compliance === "NON_COMPLIANT") {
                   annotation = "Description of why the resource is not
compliant.";
               }
               // Initializes the request that contains the evaluation results.
               if (annotation) {
                   putEvaluationsRequest = {
                       Evaluations: [{
                           // Applies the evaluation result to the AWS account
published in the event.
                           ComplianceResourceType: 'AWS::::Account',
                           ComplianceResourceId: event.accountId,
                           ComplianceType: compliance,
                           OrderingTimestamp: new Date(),
                           Annotation: annotation
                       }],
                       ResultToken: event.resultToken
                   };
               } else {
                   putEvaluationsRequest = {
                       Evaluations: [{
                           // Applies the evaluation result to the AWS account
published in the event.
                           ComplianceResourceType: 'AWS::::Account',
                           ComplianceResourceId: event.accountId,
                           ComplianceType: compliance,
                           OrderingTimestamp: new Date()
                       }],
                       ResultToken: event.resultToken
                   };
               }

               // Sends the evaluation results to AWS Config.
               try {
```

```
                    await configClient.send(new
 PutEvaluationsCommand(putEvaluationsRequest));
                }
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource
 type.", null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
```

```
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count,
 callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
}
```

함수 작업

함수는 실행 시 다음 작업을 수행합니다.

1. 함수는가 `event` 객체를 `handler` 함수에 AWS Lambda 전달할 때 실행됩니다. 이 예제에서 함수는 호출자에게 정보를 반환하는 데 사용하는 선택적 `callback` 파라미터를 수락합니다. AWS Lambda 또한 함수가 실행되는 동안 사용할 수 있는 정보와 메서드가 포함된 `context` 객체를 전달합니다. 참고로, 최신 버전의 Lambda에서는 컨텍스트가 더 이상 사용되지 않습니다.
2. 지정된 유형의 리소스 수를 세기 위해 핸들러는 `countResourceTypes` 함수를 호출한 다음, 이벤트에서 수신한 `applicableResourceType` 파라미터를 전달합니다. `countResourceTypes` 함수는 `listDiscoveredResources` 클라이언트의 `config` 메서드를 호출합니다. 그러면 해당하는 리소스의 식별자 목록이 반환됩니다. 함수는 이 목록의 길이를 사용하여 해당하는 리소스 수를 확인하고, 이 수를 핸들러에게 반환합니다.
3. 핸들러는 `putEvaluationsRequest` 객체를 초기화하여 평가 결과를 AWS Config 로 전송할 준비를 합니다. 이 객체에는 규정 준수 결과와 이벤트에 게시된를 식별하는 `Evaluations` 파라미터 AWS 계정 가 포함되어 있습니다. `Evaluations` 파라미터를 사용하여 AWS Config가 지

원하는 리소스 유형에 결과를 적용할 수 있습니다. `putEvaluationsRequest` 객체에는 규칙과 이벤트를 식별하는 이벤트의 결과 토큰도 포함됩니다 AWS Config.

4. `putEvaluationsRequest` 객체 내에서 핸들러는 `evaluateCompliance` 함수를 호출합니다. 이 함수는 해당하는 리소스 수가 이벤트에서 제공한 `maxCount` 파라미터에 할당된 최대치를 초과하는지 여부를 테스트합니다. 리소스 수가 최대치를 초과하면 함수는 `NON_COMPLIANT`를 반환합니다. 리소스 수가 최대치를 초과하지 않으면 함수는 `COMPLIANT`를 반환합니다.
5. 핸들러는 객체를 `config` 클라이언트의 `putEvaluations` 메서드에 전달 AWS Config 하여 평가 결과를에 전송합니다.

AWS Config 규칙에 대한 AWS Lambda 함수 예제(Python)

AWS Lambda 는 AWS 서비스에서 게시한 이벤트에 대한 응답으로 함수를 실행합니다. AWS Config 사용자 지정 Lambda 규칙의 함수는에서 게시한 이벤트를 수신한 다음 AWS Config이벤트에서 수신한 데이터와 AWS Config API에서 검색한 데이터를 사용하여 규칙의 규정 준수를 평가합니다. 구성 규칙의 함수 작업은 구성 변경으로 트리거된 평가를 수행하는지 주기적으로 트리거된 평가를 수행하는지에 따라 다릅니다.

AWS Lambda 함수 내의 일반적인 패턴에 대한 자세한 내용은 AWS Lambda 개발자 안내서의 프로그래밍 모델을 참조하세요.

Example Function for Evaluations Triggered by Configuration Changes

AWS Config 는 사용자 지정 규칙의 범위 내에 있는 리소스에 대한 구성 변경을 감지하면 다음 예제와 같은 함수를 호출합니다.

AWS Config 콘솔을 사용하여이 예제와 같은 함수와 연결된 규칙을 생성하는 경우 트리거 유형으로 구성 변경을 선택합니다. AWS Config API 또는를 사용하여 규칙을 AWS CLI 생성하는 경우 `MessageType` 속성을 `ConfigurationItemChangeNotification` 및 로 설정합니다`OversizedConfigurationItemChangeNotification`. 이러한 설정을 사용하면가 리소스 변경으로 인해 구성 항목 또는 크기 초과 구성 항목을 AWS Config 생성할 때마다 규칙을 트리거할 수 있습니다.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
```

```
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
```

```
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] =
 json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'],
 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
```

```
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
```

```
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
       ],
       ResultToken=event['resultToken'])
```

함수 작업

함수는 실행 시 다음 작업을 수행합니다.

1. 함수는가 `event` 객체를 `handler` 함수에 AWS Lambda 전달할 때 실행됩니다. 이 예제에서 함수는 호출자에게 정보를 반환하는 데 사용하는 선택적 `callback` 파라미터를 수락합니다. AWS Lambda 또한 함수가 실행되는 동안 사용할 수 있는 정보와 메서드가 포함된 `context` 객체를 전달합니다. 참고로, 최신 버전의 Lambda에서는 컨텍스트가 더 이상 사용되지 않습니다.
2. 함수는 이벤트의 `messageType`이 구성 항목인지 크기를 초과한 구성 항목인지 확인한 다음, 해당 구성 항목을 반환합니다.
3. 핸들러는 `isApplicable` 함수를 호출하여 리소스가 삭제되었는지 여부를 확인합니다.

   > **Note**
   >
   > 삭제된 리소스에 대해 보고하는 규칙은 불필요한 규칙 평가를 피하기 위해 `NOT_APPLICABLE` 평가 결과를 반환해야 합니다.

4. 핸들러는 `evaluateChangeNotificationCompliance` 함수를 호출하고 이벤트에 AWS Config 게시된 `configurationItem` 및 `ruleParameters` 객체를 전달합니다.

   함수는 먼저 리소스가 EC2 인스턴스인지 여부를 평가합니다. 리소스가 EC2 인스턴스가 아닌 경우, 함수는 준수 값 `NOT_APPLICABLE`을 반환합니다.

그런 다음 함수는 구성 항목의 `instanceType` 속성이 `desiredInstanceType` 파라미터 값과 같은지 여부를 평가합니다. 값이 같으면 함수는 `COMPLIANT`를 반환합니다. 값이 같지 않으면 함수는 `NON_COMPLIANT`를 반환합니다.

5. 핸들러는 `putEvaluationsRequest` 객체를 초기화하여 평가 결과를 AWS Config 로 전송할 준비를 합니다. 이 객체에는 준수 결과를 식별하는 `Evaluations` 파라미터, 리소스 유형, 평가된 리소스의 ID가 포함되어 있습니다. `putEvaluationsRequest` 객체에는 규칙과 이벤트를 식별하는 이벤트의 결과 토큰도 포함됩니다 AWS Config.
6. 핸들러는 객체를 `config` 클라이언트의 `putEvaluations` 메서드에 전달 AWS Config 하여 평가 결과를에 전송합니다.

Example Function for Periodic Evaluations

AWS Config 는 정기 평가를 위해 다음 예제와 같은 함수를 호출합니다. 주기적 평가는 사용자가 AWS Config에서 규칙을 정의할 때 지정한 간격으로 발생합니다.

AWS Config 콘솔을 사용하여이 예제와 같은 함수와 연결된 규칙을 생성하는 경우 트리거 유형으로 주기적을 선택합니다. AWS Config API 또는를 사용하여 규칙을 AWS CLI 생성하는 경우 `MessageType` 속성을 로 설정합니다`ScheduledNotification`.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
```

```
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value
 to the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
```

```
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled
 rules.
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report
 on the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])
        valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
```

```
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
count_resource_types(valid_rule_parameters['applicableResourceType'], '',
resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
ResultToken=event['resultToken'])
```

함수 작업

함수는 실행 시 다음 작업을 수행합니다.

1. 함수는가 `event` 객체를 `handler` 함수에 AWS Lambda 전달할 때 실행됩니다. 이 예제에서 함수는 호출자에게 정보를 반환하는 데 사용하는 선택적 `callback` 파라미터를 수락합니다. AWS Lambda 또한 함수가 실행되는 동안 사용할 수 있는 정보와 메서드가 포함된 `context` 객체를 전달합니다. 참고로, 최신 버전의 Lambda에서는 컨텍스트가 더 이상 사용되지 않습니다.
2. 지정된 유형의 리소스 수를 세기 위해 핸들러는 `countResourceTypes` 함수를 호출한 다음, 이벤트에서 수신한 `applicableResourceType` 파라미터를 전달합니다. `countResourceTypes` 함수는 `listDiscoveredResources` 클라이언트의 `config` 메서드를 호출합니다. 그러면 해당하는 리소스의 식별자 목록이 반환됩니다. 함수는 이 목록의 길이를 사용하여 해당하는 리소스 수를 확인하고, 이 수를 핸들러에게 반환합니다.
3. 핸들러는 `putEvaluationsRequest` 객체를 초기화하여 평가 결과를 AWS Config 로 전송할 준비를 합니다. 이 객체에는 규정 준수 결과와 이벤트에 게시된를 식별하는 `Evaluations` 파라미터 AWS 계정 가 포함되어 있습니다. `Evaluations` 파라미터를 사용하여 AWS Config가 지원하는 리소스 유형에 결과를 적용할 수 있습니다. `putEvaluationsRequest` 객체에는 규칙과 이벤트를 식별하는 이벤트의 결과 토큰도 포함됩니다 AWS Config.
4. `putEvaluationsRequest` 객체 내에서 핸들러는 `evaluateCompliance` 함수를 호출합니다. 이 함수는 해당하는 리소스 수가 이벤트에서 제공한 `maxCount` 파라미터에 할당된 최대치를 초과하는지 여부를 테스트합니다. 리소스 수가 최대치를 초과하면 함수는 `NON_COMPLIANT`를 반환합니다. 리소스 수가 최대치를 초과하지 않으면 함수는 `COMPLIANT`를 반환합니다.
5. 핸들러는 객체를 `config` 클라이언트의 `putEvaluations` 메서드에 전달 AWS Config 하여 평가 결과를에 전송합니다.

AWS Config 규칙에 대한 이벤트 예제

규칙에 대한 트리거가 발생하면는 이벤트를 게시하여 규칙의 AWS Lambda 함수를 AWS Config 호출합니다. 그런 다음 함수의 핸들러에 이벤트를 전달하여 함수를 AWS Lambda 실행합니다.

Example Event for Evaluations Triggered by Configuration Changes

AWS Config 는 규칙 범위 내에 있는 리소스에 대한 구성 변경을 감지하면 이벤트를 게시합니다. 다음 이벤트 예제에서는 규칙이 EC2 인스턴스의 구성 변경으로 트리거되었음을 보여 줍니다.

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Example Event for Evaluations Triggered by Oversized Configuration Changes

일부 리소스 변경은 크기를 초과한 구성 항목을 생성합니다. 다음 이벤트 예제에서는 규칙이 EC2 인스턴스의 크기를 초과한 구성 변경으로 트리거되었음을 보여 줍니다.

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
```

```
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

Example Event for Evaluations Triggered by Periodic Frequency

AWS Config 는 사용자가 지정한 빈도(예: 24시간마다)로 리소스를 평가할 때 이벤트를 게시합니다. 다음 이벤트 예제에서는 규칙이 주기적 간격으로 트리거되었음을 보여 줍니다.

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime
\":\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",
\"recordVersion\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

이벤트 속성

AWS Config 이벤트에 대한 JSON 객체에는 다음 속성이 포함됩니다.

`invokingEvent`

규칙에 대한 평가를 트리거하는 이벤트입니다. 이벤트가 리소스 구성 변경에 대한 응답으로 게시되는 경우, 이 속성의 값은 JSON `configurationItem` 또는 `configurationItemSummary`(크기를 초과한 구성 항목의 경우)를 포함하는 문자열입니다. 구성 항목은가 변경을 AWS Config 감지한 시점의 리소스 상태를 나타냅니다. 구성 항목의 예는의 `get-resource-config-history` AWS CLI 명령에서 생성된 출력을 참조하세요구성 기록 보기.

주기적 평가에 대한 이벤트가 게시되는 경우, 값은 JSON 객체를 포함하는 문자열입니다. 객체에는 트리거된 평가에 대한 정보가 포함됩니다.

각 이벤트 유형에 대해 함수는 문자열의 콘텐츠를 평가할 수 있도록 다음 Node.js 예와 같이 JSON 구문 분석기로 문자열을 구문 분석해야 합니다.

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

함수가 평가 논리의 일부로 처리하는 키/값 페어입니다. AWS Config 콘솔을 사용하여 사용자 지정 Lambda 규칙을 생성할 때 파라미터를 정의합니다. `PutConfigRule` AWS Config API 요청 또는 `put-config-rule` AWS CLI 명령의 `InputParameters` 속성을 사용하여 파라미터를 정의할 수도 있습니다.

파라미터의 JSON 코드는 문자열 안에 포함되어 있으므로, 함수는 문자열의 콘텐츠를 평가할 수 있도록 다음 Node.js 예와 같이 JSON 구문 분석기로 문자열을 구문 분석해야 합니다.

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

함수가 `PutEvaluations` 호출을 AWS Config 통해 전달해야 하는 토큰입니다.

`eventLeftScope`

평가할 AWS 리소스가 규칙 범위에서 제거되었는지 여부를 나타내는 부울 값입니다. 값이 `true`이면 함수는 `NOT_APPLICABLE` 호출에서 `ComplianceType`을 `PutEvaluations` 속성의 값으로 전달하여 평가를 무시할 수 있음을 나타냅니다.

`executionRoleArn`

할당된 IAM 역할의 ARN입니다 AWS Config.

`configRuleArn`

가 규칙에 AWS Config 할당한 ARN입니다.

`configRuleName`

에서 이벤트를 AWS Config 게시하고 함수를 호출하도록 규칙에 할당한 이름입니다.

`configRuleId`

가 규칙에 AWS Config 할당한 ID입니다.

`accountId`

규칙을 소유 AWS 계정 한의 ID입니다.

`version`

에서 할당한 버전 번호입니다 AWS. 가 AWS Config 이벤트에 속성을 추가하면 AWS 버전이 증가합니다. 함수에 특정 버전과 일치하거나 이를 초과하는 이벤트에만 있는 속성이 필요한 경우, 해당 함수가 이 속성의 값을 확인할 수 있습니다.

AWS Config 이벤트의 현재 버전은 1.0입니다.

AWS Config 사용자 지정 Lambda 규칙을 사용하여 삭제된 리소스 관리

삭제된 리소스에 대해 보고하는 규칙은 불필요한 규칙 평가를 피하기 위해 `NOT_APPLICABLE` 평가 결과를 반환해야 합니다.

리소스를 삭제하면가에 `ResourceDeleted` 대해를 `configurationItem` 사용하여를 AWS Config 생성합니다`configurationItemStatus`. 이 메타데이터를 사용하여 규칙이 삭제된 리소스를 보고하는지 확인할 수 있습니다. 구성 항목에 대한 자세한 내용은 개념 | 구성 항목을 참조하세요.

다음 코드 조각을 포함하여 삭제된 리소스를 확인하고 삭제된 리소스에 대해 보고하는 `NOT_APPLICABLE` 경우 AWS Config 사용자 지정 Lambda 규칙의 평가 결과를 로 설정합니다.

Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
```

```
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

> **Note**
>
> AWS Config 관리형 규칙 및 AWS Config 사용자 지정 정책 규칙은 기본적으로이 동작을 처리합니다.
>
> AWS Config Development Kit(RDK) 및 AWS Config Development Kit Library(RDKlib)를 사용하여 Python으로 AWS Config 사용자 지정 Lambd 규칙을 생성하는 경우 가져온 평가자 클래스가이 동작을 확인합니다. RDK 및 RDKlib를 사용하여 규칙을 작성하는 방법에 대한 자세한 내용은 RDK 및 RDKlib를 사용하여 규칙 작성을 참조하세요.

서비스 연결 AWS Config 규칙

서비스 연결 AWS Config 규칙은 계정에서 규칙을 생성하기 위해 다른 AWS 서비스를 지원하는 고유한 유형의 AWS Config 관리형 AWS Config 규칙입니다. 서비스 연결 규칙은 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함하도록 사전 정의되어 있습니다. 이러한 규칙은 AWS 서비스에서 규정 준수 확인을 AWS 계정 위해에서 권장하는 표준과 유사합니다.

이러한 서비스 연결 AWS Config 규칙은 AWS 서비스 팀이 소유합니다. AWS 서비스 팀은에서 이러한 규칙을 생성합니다 AWS 계정. 이러한 규칙에 대해서는 읽기 전용 액세스만 제공됩니다. 이러한 규칙이 연결된 AWS 서비스를 구독하는 경우 이러한 규칙을 편집하거나 삭제할 수 없습니다.

서비스 연결 규칙 및 AWS Command Line Interface

를 사용하면 AWS CLIPutConfigRule, DeleteConfigRule 및 DeleteEvaluationResults APIs 다음 오류 메시지와 함께 액세스 거부를 반환합니다.

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

서비스 연결 규칙 및 AWS Config 콘솔

AWS Config 콘솔의 AWS Config 규칙 페이지에 서비스 연결 규칙이 표시됩니다. 편집 및 결과 삭제 버튼은 규칙 편집을 제한하기 위해 콘솔에서 회색으로 표시됩니다. 규칙을 선택하여 규칙 세부 정보를 볼 수 있습니다.

서비스 연결 규칙, 해결 작업 및 적합성 팩

적합성 팩의 서비스 연결 규칙에 수정 작업을 추가하려면 적합성 팩 템플릿 자체에 문제 해결 작업을 추가한 다음 업데이트된 템플릿으로 적합성 팩을 업데이트해야 합니다. 적합성 팩 업데이트에 대한 자세한 내용은 적합성 팩 배포(콘솔), 적합성 팩 배포(AWS CLI) 및 조직 적합성 팩 관리를 참조하세요.

서비스 연결 규칙 편집 및 삭제

서비스 연결 규칙을 편집하거나 삭제하려면 규칙을 생성한 AWS 서비스에 문의하세요. 예를 들어에서 생성한 서비스 연결 규칙의 경우 AWS Security Hub 사용 설명서: 보안 표준 비활성화의 다음 단계에 따라 서비스 연결 규칙을 제거할 AWS Security Hub수 있습니다. https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-enable-disable.html

조직의 모든 계정에서 AWS Config 규칙 관리

> **Important**
>
> 조직 규칙은 API 또는 CLI API로만 생성할 수 있습니다. AWS Config 콘솔에서는이 작업이 지원되지 않습니다.

AWS Config 를 사용하면 조직 AWS 계정 내 모든에서 AWS Config 규칙을 관리할 수 있습니다. 다음을 할 수 있습니다.

- 조직의 모든 계정에서 AWS Config 규칙을 중앙에서 생성, 업데이트 및 삭제합니다.
- 모든 계정에 공통 규칙 세트를 배포하고 AWS Config 규칙을 생성해서는 AWS Config 안 되는 계정을 지정합니다.
- 의 관리 계정에서 APIs AWS Organizations 를 사용하여 조직의 멤버 계정에서 기본 AWS Config 규칙을 수정할 수 없도록 하여 거버넌스를 적용합니다.

고려 사항

여러 리전에 배포하는 경우

계정 간에 규칙 및 적합성 팩을 배포하기 위한 API 호출은 AWS 리전별로 다릅니다. 규칙을 다른 리전에 배포하려면 조직 수준에서 API 직접 호출의 컨텍스트를 다른 리전으로 변경해야 합니다. 예를 들어 미국 동부(버지니아 북부)에 규칙을 배포하려면 리전을 미국 동부(버지니아 북부)로 변경한 다음 `PutOrganizationConfigRule`을 직접적으로 호출합니다.

조직 내 계정의 경우

새 계정이 조직에 가입하면 규칙 또는 적합성 팩이 해당 계정에 배포됩니다. 계정이 조직을 나가면 규칙 또는 적합성 팩이 제거됩니다.

조직 관리자 계정에 조직 규칙 또는 적합성 팩을 배포한 다음 위임된 관리자를 설정하고 위임된 관리자 계정에 조직 규칙 또는 적합성 팩을 배포하는 경우 위임된 관리자 계정에서 조직 관리자 계정의 조직 규칙 또는 적합성 팩을 볼 수 없고 조직 관리자 계정에서 위임된 관리자 계정의 조직 규칙 또는 적합성 팩을 볼 수 없습니다. DescribeOrganizationConfigRules및 DescribeOrganizationConformancePacks API는 이러한 API를 호출하는 계정에 배포된 조직 관련 리소스만 보고 상호 작용할 수 있습니다.

조직에 추가된 새 계정에 대한 재시도 메커니즘

레코더를 사용할 수 없는 경우 조직에 계정을 추가한 후 7시간 동안만 기존 조직 규칙 및 적합성 팩 배포가 다시 시도됩니다. 조직에 계정을 추가한 후 7시간 이내에 레코더가 없으면 레코더를 생성해야 합니다.

조직 관리 계정, 위임된 관리자 및 서비스 연결 역할

조직 관리 계정을 사용 중이고 조직 배포에 위임된 관리자를 사용하려는 경우 AWS Config 가 서비스 연결 역할(SLR)을 자동으로 생성하지 않는다는 점에 유의하세요. IAM을 사용하여 별도의 서비스 연결 역할(SLR)을 수동으로 생성해야 합니다.

관리 계정에 대한 SLR이 없는 경우 위임된 관리자 계정에서 해당 계정에 리소스를 배포할 수 없습니다. 관리 및 위임된 관리자 계정에서 멤버 계정에 AWS Config 규칙을 배포할 수 있습니다. 자세한 내용은 AWS Identity and Access Management (IAM) 사용 설명서의 서비스 연결 역할 사용을 참조하세요.

배포

AWS Config 와 통합하는 방법에 대한 자세한 내용은 AWS Organizations 사용 설명서의 AWS Config 및 AWS Organizations 섹션을 AWS Organizations참조하세요. 다음 APIs를 사용하여 조직 AWS 계정 내 모든에서 AWS Config 규칙을 관리하기 전에 AWS Config 기록이 켜져 있는지 확인합니다.

- PutOrganizationConfigRule은 AWS 리소스가 원하는 구성을 준수하는지 여부를 평가하는 전체 조직에 대한 조직 구성 규칙을 추가하거나 업데이트합니다.
- DescribeOrganizationConfigRules - 조직 구성 규칙의 목록을 반환합니다.
- GetOrganizationConfigRuleDetailedStatus - 주어진 조직 구성 규칙에 대한 조직 내 각 멤버 계정의 세부 상태를 반환합니다.
- GetOrganizationCustomRulePolicy - 조직 구성 사용자 지정 정책 규칙의 논리가 포함된 정책 정의를 반환합니다.
- DescribeOrganizationConfigRuleStatuses - 조직에 대한 조직 구성 규칙 배포 상태를 제공합니다.
- DeleteOrganizationConfigRule - 지정된 조직 구성 규칙과 해당 조직의 모든 멤버 계정에서 나온 모든 평가 결과를 삭제합니다.

리전 지원

AWS 조직의 멤버 계정에 AWS Config 규칙 배포는 다음 리전에서 지원됩니다.

리전 이름	지역	엔드포인트	프로토콜
미국 동부 (오하이오)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
미국 동부 (버지니아 북부)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
미국 서부(캘리포니아 북부)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
미국 서부(오레곤)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
아프리카(케이프타운)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
아시아 태평양(홍콩)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
아시아 태평양(하이데라바드)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
아시아 태평양(자카르타)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
아시아 태평양(멜버른)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
아시아 태평양(뭄바이)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
아시아 태평양(오사카)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(서울)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
아시아 태평양(시드니)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
아시아 태평양(도쿄)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
캐나다(중부)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
캐나다 서부(캘거리)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
유럽(프랑크푸르트)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
유럽(아일랜드)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
유럽(런던)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
유럽(밀라노)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
유럽(파리)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
유럽(스페인)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
유럽(스톡홀름)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
유럽(취리히)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
이스라엘(텔아비브)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
중동(바레인)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
중동(UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
남아메리카(상파울루)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 동부)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 서부)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config 규칙 추가

AWS Config 콘솔 또는 AWS SDKs를 사용하여 규칙을 추가할 수 있습니다.

주제

- 규칙 추가(콘솔)
- 규칙(AWS SDKs) 추가

규칙 추가(콘솔)

규칙 페이지에 규칙과 각 규칙의 현재 준수 상태가 표로 표시됩니다. 가 규칙에 대한 리소스 평가를 AWS Config 완료할 때까지 각 규칙의 결과는 평가 중...입니다. 새로 고침 버튼으로 결과를 업데이트할 수 있습니다. 가 평가를 AWS Config 완료하면 규정 준수 또는 비준수 규칙과 리소스 유형을 볼 수 있습니다. 자세한 내용은 를 사용하여 AWS 리소스에 대한 규정 준수 정보 및 평가 결과 보기 AWS Config 단원을 참조하십시오.

> **Note**
>
> 새 규칙을 추가하면는 이전에 기록된 리소스를 포함하여 리소스 인벤토리의 해당 리소스를 AWS Config 평가합니다. 예를 들어 `AWS::IoT::Policy` 리소스를 기록했지만 나중에 기록에서 제외한 경우는 초기 구성 항목(CIs)을 인벤토리에 AWS Config 유지합니다. 연결된 리소스 유형이 기록에서 제외될 때는 더 이상 이러한 CIs를 업데이트 AWS Config 하지 않지만, 마지막으로 기록된 상태를 유지하고 적용 가능한 규칙을 추가할 때 평가합니다.
>
> AWS Config 는 리소스 인벤토리에 없는 리소스를 평가하지 않습니다. 예를 들어 amplify-branch-tagged 규칙을 추가하지만 `AWS::Amplify::Branch` 리소스를 기록하지 않고 기록한 적이 없는 경우 AWS Config 는 계정의 AWS Amplify 브랜치가 규정을 준수하는지 여부를 평가할 수 없습니다.
>
> 자세한 내용은 를 사용하여 AWS 리소스 기록 AWS Config 단원을 참조하십시오.

규칙 추가

규칙을 추가하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Management Console 메뉴에서 리전 선택기가 AWS Config 규칙을 지원하는 리전으로 설정되어 있는지 확인합니다. 지원되는 리전의 목록은 Amazon Web Services 일반 참조의 AWS Config 리전 및 엔드포인트를 참조하세요.
3. 왼쪽 탐색 창에서 규칙을 선택합니다.

4. 규칙 페이지에서 규칙 추가를 선택합니다.
5. 규칙 유형 지정 페이지에서 다음 단계를 완료하여 규칙 유형을 지정합니다.
   a. 검색 필드에 입력하여 규칙 이름, 설명 및 레이블을 기준으로 관리형 규칙 목록을 필터링합니다. 예를 들어 EC2를 입력하면 EC2 인스턴스 유형을 평가하는 규칙이, 주기적을 입력하면 주기적으로 트리거되는 규칙이 표시됩니다.
   b. 고유의 사용자 지정 규칙을 만들 수도 있습니다. Lambda를 사용하여 사용자 지정 규칙 생성 또는 Guard를 사용하여 사용자 지정 규칙 생성을 선택하고 사용자 AWS Config 지정 Lambda 규칙 생성 또는 AWS Config 사용자 지정 정책 규칙 생성의 절차를 따릅니다.
6. 규칙 구성 페이지에서 다음 단계를 완료하여 규칙을 구성합니다.
   a. 이름에 규칙의 고유 이름을 입력합니다.
   b. 설명에 규칙에 대한 설명을 입력합니다.
   c. 평가 모드에서 리소스 생성 및 관리 프로세스에서 리소스를 평가하려는 시기 AWS Config 를 선택합니다. 규칙에 따라는 리소스가 배포되기 전, 리소스가 배포된 후 또는 둘 다에서 리소스 구성을 평가할 AWS Config 수 있습니다.
      i. 리소스를 배포하기 전에 리소스의 구성 설정에 대한 평가를 실행하려면 사전 평가 켜기를 선택합니다.

         사전 평가를 활성화한 후에는 StartResourceEvaluation API 및 GetResourceEvaluationSummary API를 사용하여 이러한 명령에 지정한 리소스가 해당 계정의 해당 리전 사전 예방 규칙에 따라 NON_COMPLIANT 플래그가 지정되는지 확인할 수 있습니다.

         이 명령 사용에 대한 자세한 내용은 AWS Config 규칙을 사용하여 리소스 평가를 참조하세요. 사전 평가를 지원하는 관리형 규칙 목록은 평가 모드별 AWS Config 관리형 규칙 목록을 참조하세요.
      ii. 기존 리소스의 구성 설정을 평가하려면 탐지 평가 켜기를 선택합니다.

         탐지 평가의 경우 트리거에는 구성이 변경되는 경우 트리거와 주기적 트리거라는 두 가지 유형이 있습니다.

         A. 규칙의 트리거 유형에 구성 변경이 포함된 경우가 Lambda 함수를 AWS Config 호출하는 변경 범위에 대해 다음 옵션 중 하나를 지정합니다.
            - 리소스 - 지정된 리소스 유형 또는 유형 및 식별자와 일치하는 리소스가 생성, 변경 또는 삭제되는 경우.

- 태그 - 지정된 태그가 있는 리소스가 생성, 변경 또는 삭제되는 경우.
- 모든 변경 사항 -에 의해 기록된 리소스 AWS Config 가 생성, 변경 또는 삭제되는 경우.

AWS Config 는 규칙의 범위와 일치하는 리소스에 대한 변경을 감지하면 평가를 실행합니다. 범위를 사용하여 평가를 시작하는 리소스를 제한할 수 있습니다.

B. 규칙의 트리거 유형에 주기적이 포함된 경우가 Lambda 함수를 AWS Config 호출하는 빈도를 지정합니다.

d. 규칙에 파라미터가 포함된 경우 파라미터에서 제공된 키의 값을 사용자 지정할 수 있습니다. 파라미터는 리소스가 규칙을 준수한다고 간주되기 위해 준수해야 하는 속성입니다.

7. 검토 및 생성 페이지에서 모든 선택 사항을 검토한 후 AWS 계정에 규칙을 추가합니다. 규칙이 예상대로 작동하지 않는 경우, 규정 준수에 다음 중 하나가 표시될 수 있습니다.

- 보고된 결과가 없음 - 규칙을 기준으로 리소스를 AWS Config 평가했습니다. 규칙이 해당 범위의 AWS 리소스에 적용되지 않았거나, 지정된 리소스가 삭제되었거나, 평가 결과가 삭제되었습니다. 평가 결과를 받으려면 규칙을 업데이트하여 범위를 변경하거나 재평가를 선택하세요.

  규칙에서 평가 결과를 보고하지 않았을 때도 이 메시지가 나타날 수 있습니다.
- 범위에 리소스 없음 - 규칙 범위 내에 AWS 리소스가 없으므로이 규칙에 대해 기록된 리소스를 평가할 수 AWS Config 없습니다. 평가 결과를 가져오려면 규칙을 편집하고 범위를 변경하거나 설정 페이지를 사용하여 기록할 AWS Config 의 리소스를 추가합니다.
- Evaluations failed - 문제 파악에 도움이 되는 정보를 얻으려면 규칙 이름을 선택하여 세부 정보 페이지를 열고 오류 메시지를 확인하세요.

규칙(AWS SDKs) 추가

규칙 추가

다음 코드 예시는 `PutConfigRule`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS 관리형 Config 규칙을 추가하려면

다음 명령은 AWS 관리형 Config 규칙을 추가하는 JSON 코드를 제공합니다.

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

RequiredTagsForEC2Instances.json은 규칙 구성이 포함된 JSON 파일입니다.

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

ComplianceResourceTypes 속성의 경우이 JSON 코드는 범위를 AWS::EC2::Instance 유형의 리소스로 제한하므로 AWS Config는 규칙에 대해 EC2 인스턴스만 평가합니다. 규칙은 관리형 규칙이므로 Owner 속성은 AWS로 설정되고 SourceIdentifier 속성은 규칙 식별자인 REQUIRED_TAGS로 설정됩니다. InputParameters 속성의 경우 규칙에 필요한 태그 키인 CostCenter 및 Owner가 지정됩니다.

명령이 성공하면 AWS Config는 출력을 반환하지 않습니다. 규칙 구성을 확인하려면 describe-config-rules 명령을 실행하고 규칙 이름을 지정합니다.

고객 관리형 Config 규칙을 추가하는 방법

다음 명령은 고객 관리형 Config 규칙을 추가하기 위한 JSON 코드를 제공합니다.

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

InstanceTypesAreT2micro.json은 규칙 구성이 포함된 JSON 파일입니다.

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
```

```
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

`ComplianceResourceTypes` 속성의 경우이 JSON 코드는 범위를 `AWS::EC2::Instance` 유형의 리소스로 제한하므로 AWS Config는 규칙에 대해 EC2 인스턴스만 평가합니다. 이 규칙은 고객 관리형 규칙이므로 `Owner` 속성은 로 설정`CUSTOM_LAMBDA`되고 `SourceIdentifier` 속성은 AWS Lambda 함수의 ARN으로 설정됩니다. `SourceDetails` 객체가 필요합니다. `InputParameters` 속성에 지정된 파라미터는 AWS Config가 규칙을 기준으로 리소스를 평가하기 위해 Lambda 함수를 호출할 때 AWS Lambda 함수로 전달됩니다.

명령이 성공하면 AWS Config는 출력을 반환하지 않습니다. 규칙 구성을 확인하려면 describe-config-rules 명령을 실행하고 규칙 이름을 지정합니다.

- API 세부 정보는 AWS CLI 명령 참조의 PutConfigRule을 참조하세요.

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 PutConfigRule을 참조하세요.

AWS Config 규칙 업데이트

AWS Config 콘솔 또는 AWS SDKs를 사용하여 규칙을 업데이트할 수 있습니다.

주제

- 규칙 업데이트(콘솔)
- 규칙(AWS SDKs) 업데이트

규칙 업데이트(콘솔)

규칙 페이지에 규칙과 각 규칙의 현재 준수 상태가 표로 표시됩니다. 가 규칙에 대한 리소스 평가를 AWS Config 완료할 때까지 각 규칙의 결과는 평가 중...입니다. 새로 고침 버튼으로 결과를 업데이트할 수 있습니다. 가 평가를 AWS Config 완료하면 규정 준수 또는 비준수 규칙과 리소스 유형을 볼 수 있습니다. 자세한 내용은 를 사용하여 AWS 리소스에 대한 규정 준수 정보 및 평가 결과 보기 AWS Config 단원을 참조하십시오.

규칙 업데이트

규칙 업데이트

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Management Console 메뉴에서 리전 선택기가 AWS Config 규칙을 지원하는 리전으로 설정되어 있는지 확인합니다. 지원되는 리전의 목록은 Amazon Web Services 일반 참조의 AWS Config 리전 및 엔드포인트를 참조하세요.
3. 왼쪽 탐색 창에서 규칙을 선택합니다.
4. 업데이트하려는 규칙을 선택하고 규칙 편집을 선택합니다.
5. 규칙 편집 페이지에서 설정을 수정하여 규칙을 필요에 따라 변경합니다.
6. 저장을 선택합니다.

규칙(AWS SDKs) 업데이트

규칙 업데이트

이전에 추가한 규칙을 업데이트하려면 이 요청에 사용하는 `ConfigRule` 데이터 형식에 `ConfigRuleName`, `ConfigRuleId` 또는 `ConfigRuleArn`을 사용하여 규칙을 지정합니다. 규칙을 추가할 때 사용하는 것과 동일한 `PutConfigRule` 명령을 사용합니다.

다음 코드 예시는 `PutConfigRule`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS 관리형 Config 규칙을 추가하려면

다음 명령은 AWS 관리형 Config 규칙을 추가하는 JSON 코드를 제공합니다.

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json`은 규칙 구성이 포함된 JSON 파일입니다.

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

`ComplianceResourceTypes` 속성의 경우이 JSON 코드는 범위를 `AWS::EC2::Instance` 유형의 리소스로 제한하므로 AWS Config는 규칙에 대해 EC2 인스턴스만 평가합니다. 규칙은 관리형 규칙이므로 `Owner` 속성은 `AWS`로 설정되고 `SourceIdentifier` 속성은 규칙 식별자

인 REQUIRED_TAGS로 설정됩니다. InputParameters 속성의 경우 규칙에 필요한 태그 키인 CostCenter 및 Owner가 지정됩니다.

명령이 성공하면 AWS Config는 출력을 반환하지 않습니다. 규칙 구성을 확인하려면 describe-config-rules 명령을 실행하고 규칙 이름을 지정합니다.

고객 관리형 Config 규칙을 추가하는 방법

다음 명령은 고객 관리형 Config 규칙을 추가하기 위한 JSON 코드를 제공합니다.

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

InstanceTypesAreT2micro.json은 규칙 구성이 포함된 JSON 파일입니다.

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

ComplianceResourceTypes 속성의 경우이 JSON 코드는 범위를 AWS::EC2::Instance 유형의 리소스로 제한하므로 AWS Config는 규칙에 대해 EC2 인스턴스만 평가합니다. 이 규칙은 고객 관리형 규칙이므로 Owner 속성은 로 설정CUSTOM_LAMBDA되고 SourceIdentifier 속성은 AWS Lambda 함수의 ARN으로 설정됩니다. SourceDetails 객체가 필요합니다.

`InputParameters` 속성에 지정된 파라미터는 AWS Config가 규칙을 기준으로 리소스를 평가하기 위해 Lambda 함수를 호출할 때 AWS Lambda 함수로 전달됩니다.

명령이 성공하면 AWS Config는 출력을 반환하지 않습니다. 규칙 구성을 확인하려면 describe-config-rules 명령을 실행하고 규칙 이름을 지정합니다.

- API 세부 정보는 AWS CLI 명령 참조의 PutConfigRule을 참조하세요.

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
```

```
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 PutConfigRule을 참조하세요.

AWS Config 규칙 삭제

AWS Config 콘솔 또는 AWS SDKs를 사용하여 규칙을 삭제할 수 있습니다.

주제

- 고려 사항
- 규칙 삭제(콘솔)
- 규칙(AWS SDKs) 삭제

고려 사항

권장 사항: 규칙을 삭제하기 전에 **`AWS::Config::ResourceCompliance`** 리소스 유형을 기록에서 제외하는 것이 좋습니다.

규칙을 삭제하면 구성 레코더 비용에 영향을 미칠 수 `AWS::Config::ResourceCompliance` 있는 에 대한 구성 항목(CIs)이 생성됩니다. 많은 수의 리소스 유형을 평가하는 규칙을 삭제하는 경우 기록된 CI의 수가 급증할 수 있습니다.

관련 비용을 방지하려면 규칙을 삭제하기 전에 `AWS::Config::ResourceCompliance` 리소스 유형에 대한 기록을 비활성화하고 규칙이 삭제된 후 기록을 다시 활성화하도록 선택할 수 있습니다.

그러나 규칙 삭제는 비동기 프로세스이므로 완료하는 데 1시간 이상 걸릴 수 있습니다. 에 대한 기록이 비활성화된 시간 동안에는 `AWS::Config::ResourceCompliance`규칙 평가가 연결된 리소스의 기록에 기록되지 않습니다.

규칙 삭제(콘솔)

규칙 페이지에 규칙과 각 규칙의 현재 준수 상태가 표로 표시됩니다. 가 규칙에 대한 리소스 평가를 AWS Config 완료할 때까지 각 규칙의 결과는 평가 중...입니다. 새로 고침 버튼으로 결과를 업데이트할 수 있습니다. 가 평가를 AWS Config 완료하면 규정 준수 또는 비준수 규칙과 리소스 유형을 볼 수 있습니다. 자세한 내용은 [를 사용하여 AWS 리소스에 대한 규정 준수 정보 및 평가 결과 보기 AWS Config](#) 단원을 참조하십시오.

> **Note**
>
> AWS Config 는 기록 중인 리소스 유형만 평가합니다. 예를 들어 Cloudtrail 지원 규칙을 추가하지만 CloudTrail 추적 리소스 유형을 기록하지 않는 경우는 계정의 추적이 규정을 준수하는지 여부를 평가할 수 AWS Config 없습니다. 자세한 내용은 [를 사용하여 AWS 리소스 기록 AWS Config](#) 단원을 참조하십시오.

규칙 삭제

규칙 삭제

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Management Console 메뉴에서 리전 선택기가 AWS Config 규칙을 지원하는 리전으로 설정되어 있는지 확인합니다. 지원되는 리전의 목록은 Amazon Web Services 일반 참조의 [AWS Config 리전 및 엔드포인트](#)를 참조하세요.
3. 왼쪽 탐색 창에서 규칙을 선택합니다.
4. 표에서 삭제하려는 규칙을 선택합니다.
5. 작업 드롭다운 목록에서 규칙 삭제를 선택합니다.
6. 메시지가 표시되면 'Delete'(대소문자 구분)를 입력한 다음 삭제를 선택합니다.

규칙(AWS SDKs) 삭제

규칙 삭제

다음 코드 예시는 `DeleteConfigRule`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS Config 규칙을 삭제하려면

다음 명령은 이름이 인 AWS Config 규칙을 삭제합니다. `MyConfigRule`

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- API 세부 정보는 AWS CLI 명령 참조의 DeleteConfigRule을 참조하세요.

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
```

```
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 DeleteConfigRule을 참조하세요.

AWS Config 규칙에 대한 세부 정보 및 규정 준수 정보 보기

> **Important**
>
> 규정 준수 상태를 정확하게 보고하려면 `AWS::Config::ResourceCompliance` 리소스 유형을 반드시 기록해야 합니다. 자세한 내용은 AWS 리소스 기록을 참조하세요.

AWS Config 콘솔 또는 AWS SDKs를 사용하여 규칙을 볼 수 있습니다.

주제

- 규칙 확인(콘솔)
- 규칙(AWS SDKs) 보기

규칙 확인(콘솔)

규칙 페이지에 규칙과 각 규칙의 현재 준수 상태가 표로 표시됩니다. 가 규칙에 대한 리소스 평가를 AWS Config 완료할 때까지 각 규칙의 결과는 평가 중...입니다. 새로 고침 버튼으로 결과를 업데이트할 수 있습니다. 가 평가를 AWS Config 완료하면 규정 준수 또는 규정 미준수 규칙 및 리소스 유형을 볼 수 있습니다. 자세한 내용은 를 사용하여 AWS 리소스에 대한 규정 준수 정보 및 평가 결과 보기 AWS Config 단원을 참조하십시오.

> **Note**
>
> AWS Config 는 기록 중인 리소스 유형만 평가합니다. 예를 들어 Cloudtrail 지원 규칙을 추가하지만 CloudTrail 추적 리소스 유형을 기록하지 않는 경우는 계정의 추적이 규정을 준수하는지 여부를 평가할 수 AWS Config 없습니다. 자세한 내용은 를 사용하여 AWS 리소스 기록 AWS Config 단원을 참조하십시오.

규칙 보기

규칙을 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Management Console 메뉴에서 리전 선택기가 AWS Config 규칙을 지원하는 리전으로 설정되어 있는지 확인합니다. 지원되는 리전의 목록은 Amazon Web Services 일반 참조의 AWS Config 리전 및 엔드포인트를 참조하세요.
3. 왼쪽 탐색 창에서 규칙을 선택합니다.
4. 규칙 페이지에는 현재에 있는 모든 규칙이 표시됩니다 AWS 계정. 여기에는 각 규칙의 이름, 연결된 문제 해결 작업 및 규정 준수 상태가 나열됩니다.
   - 규칙 추가를 선택하여 규칙 생성을 시작합니다.
   - 규칙을 선택하여 해당 설정을 보거나 규칙을 선택하고 세부 정보 보기 선택합니다.
   - 규칙이 리소스를 평가할 때 해당 규칙의 준수 상태를 확인합니다.
   - 규칙을 선택하고 규칙 편집을 선택하여 규칙의 구성 설정을 변경하고 규정 미준수 규칙에 대한 문제 해결 작업을 설정합니다.

규칙(AWS SDKs) 보기

규칙에 대한 세부 정보 확인

다음 코드 예시는 `DescribeConfigRules`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS Config 규칙에 대한 세부 정보를 가져오는 방법

다음 명령은 이름이 인 AWS Config 규칙에 대한 세부 정보를 반환합니다. `InstanceTypesAreT2micro`

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

출력:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeConfigRules를 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 샘플에는 선택한 속성과 함께 계정에 대한 구성 규칙이 나열되어 있습니다.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

출력:

```
ConfigRuleName                                   ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                   ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                            config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                              config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required       config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조(V4)의 DescribeConfigRules를 참조하세요.

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class ConfigWrapper:
```

```
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 DescribeConfigRules을 참조하세요.

규칙에 대한 규정 준수 정보 확인

다음 코드 예시는 `DescribeComplianceByConfigRule`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS Config 규칙에 대한 규정 준수 정보를 가져오는 방법

다음 명령은 하나 이상의 AWS 리소스에서 위반한 각 AWS Config 규칙에 대한 규정 준수 정보를 반환합니다.

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

출력에서 각 `CappedCount` 속성의 값은 관련 규칙을 준수하지 않는 리소스 수를 나타냅니다. 예를 들어 다음 출력은 3개의 리소스가 `InstanceTypesAreT2micro`라는 규칙을 준수하지 않음을 나타냅니다.

출력:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeComplianceByConfigRule 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제는 규칙에 대한 현재 평가 결과가 없으므로 INSUFFICIENT_DATA를 반환하는 규칙 ebs-optimized-instance에 대한 규정 준수 세부 정보를 검색합니다.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

출력:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

예제 2: 이 예제는 규칙 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK에 대한 비준수 리소스 수를 반환합니다.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

출력:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- API 세부 정보는 Cmdlet 참조(V4)의 DescribeComplianceByConfigRule을 참조하세요. AWS Tools for PowerShell

규칙에 대한 규정 준수 요약 확인

다음 코드 예시는 `GetComplianceSummaryByConfigRule`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS Config 규칙에 대한 규정 준수 요약을 가져오는 방법

다음 명령은 규정을 준수하는 규칙의 수와 규정을 미준수하는 규칙의 수를 반환합니다.

```
aws configservice get-compliance-summary-by-config-rule
```

출력에서 각 `CappedCount` 속성의 값은 규정 준수 또는 규정 미준수 규칙의 수를 나타냅니다.

출력:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- API 세부 정보는 AWS CLI 명령 참조의 GetComplianceSummaryByConfigRule 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 샘플은 규정을 준수하지 않는 Config 규칙 수를 반환합니다.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

출력:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- API 세부 정보는 Cmdlet 참조(V4)의 GetComplianceSummaryByConfigRule을 참조하세요. AWS Tools for PowerShell

규칙에 대한 평가 결과 확인

다음 코드 예시는 `GetComplianceDetailsByConfigRule`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS Config 규칙에 대한 평가 결과를 가져오는 방법

다음 명령은 라는 AWS Config 규칙을 준수하지 않는 모든 리소스에 대한 평가 결과를 반환합니다`InstanceTypesAreT2micro`.

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

출력:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
```

```
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 GetComplianceDetailsByConfigRule 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제는 규칙 access-keys-rotated에 대한 평가 결과를 얻고 규정 준수 유형별로 그룹화된 출력을 반환합니다.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

출력:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

예제 2: 이 예제는 COMPLIANT 리소스에 대한 규칙 access-keys-rotated에 대한 규정 준수 세부 정보를 쿼리합니다.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

출력:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- API 세부 정보는 Cmdlet 참조(V4)의 GetComplianceDetailsByConfigRule을 참조하세요. AWS Tools for PowerShell

AWS Config 규칙에 대한 사전 평가 켜기

AWS Config 콘솔 또는 AWS SDKs를 사용하여 사전 평가 규칙을 켤 수 있습니다. 사전 평가를 지원하는 리소스 유형 및 관리형 규칙 목록은 규칙의 구성 요소 | 평가 모드를 참조하세요.

주제

- 사전 평가 활성화(콘솔)
- 사전 평가(AWS SDKs) 켜기

사전 평가 활성화(콘솔)

규칙 페이지에 규칙과 각 규칙의 현재 준수 상태가 표로 표시됩니다. 가 규칙에 대한 리소스 평가를 AWS Config 완료할 때까지 각 규칙의 결과는 평가 중...입니다. 새로 고침 버튼으로 결과를 업데이트할 수 있습니다.

가 평가를 AWS Config 완료하면 규정 준수 또는 규정 미준수 규칙 및 리소스 유형을 볼 수 있습니다. 자세한 내용은 를 사용하여 AWS 리소스에 대한 규정 준수 정보 및 평가 결과 보기 AWS Config 단원을 참조하십시오.

> **Note**
>
> AWS Config 는 기록 중인 리소스 유형만 평가합니다. 예를 들어 Cloudtrail 지원 규칙을 추가하지만 CloudTrail 추적 리소스 유형을 기록하지 않는 경우는 계정의 추적이 규정을 준수하는지 여부를 평가할 수 AWS Config 없습니다. 자세한 내용은 를 사용하여 AWS 리소스 기록 AWS Config 단원을 참조하십시오.

사전 평가 활성화

사전 평가를 사용하여 리소스를 배포하기 전에 리소스를 평가할 수 있습니다. 이렇게 하면 리전의 계정에 있는 선제적 규칙 세트를 고려하여 리소스 속성 세트를 사용하여 AWS 리소스를 정의하는 경우 COMPLIANT 또는 NON_COMPLIANT인지 평가할 수 있습니다.

리소스 유형 스키마는 리소스의 속성을 명시합니다. 리소스 유형 스키마는 AWS CloudFormation 레지스트리 내 또는 다음 CLI 명령으로 "AWS 퍼블릭 확장"에서 찾을 수 있습니다.

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation 레지스트리를 통한 확장 관리 및 AWS 리소스 및 속성 유형 참조를 참조하세요.

> **Note**
>
> 사전 예방 규칙은 NON_COMPLIANT로 플래그가 지정된 리소스를 수정하거나 배포를 금지하지 않습니다.

사전 평가를 활성화하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Management Console 메뉴에서 리전 선택기가 AWS Config 규칙을 지원하는 리전으로 설정되어 있는지 확인합니다. 지원되는 AWS 리전의 목록은 Amazon Web Services 일반 참조의 AWS Config 리전 및 엔드포인트를 참조하세요.
3. 왼쪽 탐색 창에서 규칙을 선택합니다. 사전 평가를 지원하는 관리형 규칙 목록은 평가 모드별 AWS Config 관리형 규칙 목록을 참조하세요.
4. 업데이트하려는 규칙을 선택하고 규칙 편집을 선택합니다.
5. 리소스를 배포하기 전에 리소스의 구성 설정에 대한 평가를 실행하려면 평가 모드에서 사전 평가 켜기를 선택합니다.
6. 저장을 선택합니다.

사전 평가를 활성화한 후에는 StartResourceEvaluation API 및 GetResourceEvaluationSummary API를 사용하여 이러한 명령에 지정한 리소스가 해당 계정의 해당 리전 사전 예방 규칙에 따라 NON_COMPLIANT 플래그가 지정되는지 확인할 수 있습니다.

예를 들어, 먼저 StartResourceEvaluation API를 사용합니다.

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

출력이 `ResourceEvaluationId`를 제공합니다.

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

그러면 `ResourceEvaluationId`를 GetResourceEvaluationSummary API와 함께 사용하여 평가 결과를 확인합니다.

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

다음과 유사한 출력 화면이 표시될 것입니다.

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

리소스에 규정 미준수 플래그를 지정한 규칙 등 평가 결과에 대한 추가 정보를 보려면 GetComplianceDetailsByResource API를 사용하세요.

사전 평가(AWS SDKs) 켜기

사전 평가 활성화(AWS CLI)

사전 평가를 사용하여 리소스를 배포하기 전에 리소스를 평가할 수 있습니다. 이렇게 하면 리전의 계정에 있는 선제적 규칙 세트를 고려하여 리소스 속성 세트를 사용하여 AWS 리소스를 정의하는 경우 COMPLIANT 또는 NON_COMPLIANT인지 평가할 수 있습니다.

리소스 유형 스키마는 리소스의 속성을 명시합니다. AWS CloudFormation 레지스트리 내 또는 다음 CLI 명령으로 "AWS 퍼블릭 확장"에서 리소스 유형 스키마를 찾을 수 있습니다.

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation 레지스트리를 통한 확장 관리 및 AWS 리소스 및 속성 유형 참조를 참조하세요.

> **Note**
> 사전 예방 규칙은 NON_COMPLIANT로 플래그가 지정된 리소스를 수정하거나 배포를 금지하지 않습니다.

사전 평가를 활성화하려면

put-config-rule 명령을 사용하고 `EvaluationModes`에서 `PROACTIVE`를 활성화합니다.

사전 평가를 켠 후에는 start-resource-evaluation CLI 명령과 get-resource-evaluation-summary CLI 명령을 사용하여 이러한 명령에 지정한 리소스가 해당 계정의 해당 리전 사전 예방 규칙에 따라 규정 미준수로 플래그가 지정되는지 확인할 수 있습니다.

예를 들어, 먼저 start-resource-evaluation 명령을 사용합니다.

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

출력이 `ResourceEvaluationId`를 제공합니다.

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

그런 다음 `ResourceEvaluationId`를 get-resource-evaluation-summary와 함께 사용하여 평가 결과를 확인합니다.

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

다음과 유사한 출력 화면이 표시될 것입니다.

```
{
```

```
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

리소스에 규정 미준수 플래그를 지정한 규칙 등 평가 결과에 대한 추가 정보를 보려면 get-compliance-details-by-resource CLI 명령을 사용하세요.

> **Note**
>
> 사전 평가를 지원하는 관리형 규칙 목록은 평가 모드별 AWS Config 관리형 규칙 목록을 참조하세요.

사전 평가 활성화(API)

사전 평가를 사용하여 리소스를 배포하기 전에 리소스를 평가할 수 있습니다. 이렇게 하면 리전의 계정에 있는 선제적 규칙 세트를 고려하여 리소스 속성 세트를 사용하여 AWS 리소스를 정의하는 경우 COMPLIANT 또는 NON_COMPLIANT인지 평가할 수 있습니다.

리소스 유형 스키마는 리소스의 속성을 명시합니다. 리소스 유형 스키마는 AWS CloudFormation 레지스트리 내 또는 다음 CLI 명령으로 "AWS 퍼블릭 확장"에서 찾을 수 있습니다.

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation 레지스트리를 통한 확장 관리 및 AWS 리소스 및 속성 유형 참조를 참조하세요.

> **Note**
> 사전 예방 규칙은 NON_COMPLIANT로 플래그가 지정된 리소스를 수정하거나 배포를 금지하지 않습니다.

규칙에서 사전 평가를 활성화하려면

PutConfigRule 작업을 사용하고 `EvaluationModes`에서 `PROACTIVE`를 활성화합니다.

사전 평가를 활성화한 후에는 StartResourceEvaluation API 및 GetResourceEvaluationSummary API를 사용하여 이러한 명령에 지정한 리소스가 해당 계정의 해당 리전 사전 예방 규칙에 따라 NON_COMPLIANT 플래그가 지정되는지 확인할 수 있습니다. 예를 들어, 먼저 StartResourceEvaluation API를 사용합니다.

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

출력이 `ResourceEvaluationId`를 제공합니다.

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

그러면 `ResourceEvaluationId`를 GetResourceEvaluationSummary API와 함께 사용하여 평가 결과를 확인합니다.

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

다음과 유사한 출력 화면이 표시될 것입니다.

```
{
```

```
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

리소스에 규정 미준수 플래그를 지정한 규칙 등 평가 결과에 대한 추가 정보를 보려면 GetComplianceDetailsByResource API를 사용하세요.

> **Note**
>
> 사전 평가를 지원하는 관리형 규칙 목록은 평가 모드별 AWS Config 관리형 규칙 목록을 참조하세요.

규칙 평가를 Security Hub로 전송

AWS Config 규칙을 추가한 후 규칙 평가를 보낼 수도 있습니다 AWS Security Hub. AWS Config 와 Security Hub 간의 통합을 통해 다른 잘못된 구성 및 보안 문제와 함께 규칙 평가를 분류하고 수정할 수 있습니다.

규칙 평가를 Security Hub로 전송

규칙 평가를 Security Hub로 보내려면 먼저 AWS Security Hub 및를 설정한 AWS Config다음 하나 이상의 AWS Config 관리형 또는 사용자 지정 규칙을 추가해야 합니다. 그런 다음 AWS Config 즉시 Security Hub로 규칙 평가 전송을 시작합니다. Security Hub는 규칙 평가를 보강하고 이를 Security Hub 조사 결과로 변환합니다.

이 통합에 대한 자세한 내용은 AWS Security Hub 사용 설명서의 사용 가능한 AWS 서비스 통합을 참조하세요.

AWS Config 규칙을 사용하여 리소스 평가

사용자 지정 규칙을 생성하거나 관리형 규칙을 사용하는 경우는 해당 규칙을 기준으로 리소스를 AWS Config 평가합니다. 규칙을 기준으로 리소스에 대한 요청 시 평가를 실행할 수 있습니다. 예를 들어 사용자 지정 규칙을 생성하고 AWS Config 가 리소스를 올바르게 평가하고 있는지 확인하거나 AWS Lambda 함수의 평가 로직에 문제가 있는지 확인하려는 경우에 유용합니다.

예제

1. IAM 사용자에게 활성 액세스 키가 있는지 여부를 평가하는 사용자 지정 규칙을 작성합니다.
2. AWS Config 는 사용자 지정 규칙을 기준으로 리소스를 평가합니다.
3. 계정에 활성 액세스 키가 없는 IAM 사용자가 있습니다. 규칙이 이 리소스를 규정 미준수로 올바르게 표시하지 않습니다.
4. 규칙을 수정한 후 평가를 다시 시작합니다.
5. 규칙을 수정했기 때문에 규칙이 리소스를 올바르게 평가하고 IAM 사용자 리소스를 규정 미준수로 표시합니다.

계정에 규칙을 추가할 때 리소스 생성 및 관리 프로세스에서 리소스를 평가할 시기 AWS Config 를 지정할 수 있습니다. 리소스 생성 및 관리 프로세스를 리소스 프로비저닝이라고 합니다. 이 프로세스에서 리소스를 평가할 시기 AWS Config 를 지정할 평가 모드를 선택합니다.

규칙에 따라는 리소스가 배포되기 전, 리소스가 배포된 후 또는 둘 다에서 리소스 구성을 평가할 AWS Config 수 있습니다. 리소스를 배포하기 전에 평가하는 것은 사전 평가입니다. 리소스를 배포한 이후에 평가하는 것은 탐지 평가합니다.

사전 예방 모드

리소스를 배포하기 전에 평가하려면 사전 평가를 사용합니다. 이를 통해 리소스 속성 세트를 사용하여 리소스를 정의하는 경우 해당 리전의 계정에 있는 사전 예방 규칙 세트를 고려하여 AWS 리소스 속성 세트가 COMPLIANT인지 NON_COMPLIANT인지 평가할 수 있습니다.

리소스 유형 스키마는 리소스의 속성을 명시합니다. AWS CloudFormation 레지스트리 내에서 또는 다음 CLI 명령을 사용하여 "AWS 퍼블릭 확장"에서 리소스 유형 스키마를 찾을 수 있습니다.

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation 레지스트리를 통한 확장 관리 및 AWS 리소스 및 속성 유형 참조를 참조하세요.

> **Note**
>
> 사전 예방 규칙은 NON_COMPLIANT로 플래그가 지정된 리소스를 수정하거나 배포를 금지하지 않습니다.

리소스 평가

사전 평가를 활성화하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Management Console 메뉴에서 리전 선택기가 AWS Config 규칙을 지원하는 리전으로 설정되어 있는지 확인합니다. 지원되는 AWS 리전의 목록은 Amazon Web Services 일반 참조의 AWS Config 리전 및 엔드포인트를 참조하세요.
3. 왼쪽 탐색 창에서 규칙을 선택합니다. 사전 평가를 지원하는 관리형 규칙 목록은 평가 모드별 AWS Config 관리형 규칙 목록을 참조하세요.
4. 업데이트하려는 규칙을 선택하고 규칙 편집을 선택합니다.
5. 리소스를 배포하기 전에 리소스의 구성 설정에 대한 평가를 실행하려면 평가 모드에서 사전 평가 켜기를 선택합니다.
6. 저장을 선택합니다.

> **Note**
>
> 또한 `put-config-rule` 명령을 사용하고 `EvaluationModes`에서 `PROACTIVE`를 활성화하거나 PutConfigRule 작업을 사용하고 `EvaluationModes`에서 `PROACTIVE`를 활성화하여 사전 평가를 활성화할 수도 있습니다.

사전 평가를 활성화한 후에는 StartResourceEvaluation API 및 GetResourceEvaluationSummary API를 사용하여 이러한 명령에 지정한 리소스가 해당 계정의 해당 리전 사전 예방 규칙에 따라 NON_COMPLIANT 플래그가 지정되는지 확인할 수 있습니다.

예를 들어, 먼저 StartResourceEvaluation API를 사용합니다.

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
```

```
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

출력이 `ResourceEvaluationId`를 제공합니다.

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

그러면 `ResourceEvaluationId`를 GetResourceEvaluationSummary API와 함께 사용하여 평가 결과를 확인합니다.

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

다음과 유사한 출력 화면이 표시될 것입니다.

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

리소스에 규정 미준수 플래그를 지정한 규칙 등 평가 결과에 대한 추가 정보를 보려면 GetComplianceDetailsByResource API를 사용하세요.

탐지 모드

이미 배포된 리소스를 평가하려면 탐지 평가를 사용합니다. 이를 통해 기존 리소스의 구성 설정을 평가할 수 있습니다.

리소스(콘솔) 평가

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Management Console 메뉴에서 리전 선택기가 AWS Config 규칙을 지원하는 리전으로 설정되어 있는지 확인합니다. 지원되는 리전의 목록은 Amazon Web Services 일반 참조의 AWS Config 리전 및 엔드포인트를 참조하세요.
3. 탐색 창에서 규칙을 선택합니다. 규칙 페이지에는 각 규칙의 이름, 관련 문제 해결 작업 및 규정 준수 상태가 표시됩니다.
4. 표에서 규칙을 선택합니다.
5. 작업 드롭다운 목록에서 재평가를 선택합니다.
6. AWS Config 는 규칙을 기준으로 리소스 평가를 시작합니다.

> **Note**
>
> 분당 한 번씩 규칙을 재평가할 수 있습니다. 다른 평가를 시작하기 전에가 규칙에 대한 평가를 AWS Config 완료할 때까지 기다려야 합니다. 규칙이 업데이트 중이거나 삭제 중인 경우 동시에 평가를 실행할 수 없습니다.

리소스(CLI) 평가

- start-config-rules-evaluation 명령을 사용합니다.

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName
```

AWS Config 는 규칙에 대해 기록된 리소스 구성을 평가하기 시작합니다. 요청에 여러 규칙을 지정할 수도 있습니다.

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

리소스(API) 평가

StartConfigRulesEvaluation 작업을 사용합니다.

AWS Config 규칙에서 평가 결과 삭제

가 규칙을 AWS Config 평가한 후 규칙 페이지 또는 규칙에 대한 규칙 세부 정보 페이지에서 평가 결과를 볼 수 있습니다. 평가 결과가 잘못되었거나 다시 평가하고 싶은 경우, 해당 규칙의 현재 평가 결과를 삭제할 수 있습니다. 예를 들어, 규칙이 리소스를 잘못 평가했거나 최근에 계정에서 리소스를 삭제한 경우, 평가 결과를 삭제하고 새 평가를 실행할 수 있습니다.

Deleting Evaluation Results (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Management Console 메뉴에서 리전 선택기가 AWS Config 규칙을 지원하는 AWS 리전으로 설정되어 있는지 확인합니다. 지원되는 리전의 목록은 Amazon Web Services 일반 참조의 AWS Config 리전 및 엔드포인트를 참조하세요.
3. 탐색 창에서 규칙을 선택합니다. 규칙 페이지에는 각 규칙의 이름, 관련 문제 해결 작업 및 규정 준수 상태가 표시됩니다.
4. 표에서 규칙을 선택합니다.
5. 작업 드롭다운 목록에서 결과 삭제를 선택합니다.
6. 메시지가 표시되면 삭제를 입력(이 입력은 대소문자를 구분)한 다음 삭제를 선택합니다. 삭제한 평가는 검색할 수 없습니다.
7. 평가 결과를 삭제한 후 새 평가를 수동으로 시작할 수 있습니다.

Deleting Evaluation Results (CLI)

- delete-evaluation-results 명령을 사용합니다.

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

  AWS Config 는 규칙에 대한 평가 결과를 삭제합니다.

Deleting Evaluation Results (API)

DeleteEvaluationResults 작업을 사용합니다.

AWS Config 규칙 문제 해결

AWS Config 규칙을 삭제할 수 없거나 "오류가 발생했습니다."라는 오류 메시지가 표시되는 경우 문제를 해결합니다 AWS Config.

AWS Identity and Access Management (IAM) 엔터티에는 DeleteConfigRule API에 대한 권한이 있습니다.

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자 또는 역할을 선택합니다.
3. AWS Config 규칙을 삭제하는 데 사용한 사용자 또는 역할을 선택하고 권한 정책을 확장합니다.
4. 권한 탭에서 JSON을 선택합니다.
5. JSON 미리 보기 창에서 IAM 정책이 DeleteConfigRule API에 대한 권한을 허용하는지 확인합니다.

IAM 엔터티 권한 경계는 DeleteConfigRule API를 허용합니다.

IAM 엔터티에 권한 경계가 있는 경우 DeleteConfigRule API에 대한 권한을 허용하는지 확인합니다.

1. https://console.aws.amazon.com/iam/에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자 또는 역할을 선택합니다.
3. AWS Config 규칙을 삭제하는 데 사용한 사용자 또는 역할을 선택하고 권한 경계를 확장한 다음 JSON을 선택합니다.
4. JSON 미리 보기 창에서 IAM 정책이 DeleteConfigRule API에 대한 권한을 허용하는지 확인합니다.

> **Warning**
>
> IAM 사용자는 장기 자격 증명을 가지므로 보안 위험이 있습니다. 이 위험을 줄이려면 이러한 사용자에게 작업을 수행하는 데 필요한 권한만 제공하고 더 이상 필요하지 않을 경우 이러한 사용자를 제거하는 것이 좋습니다.

서비스 제어 정책(SCP)은 DeleteConfigRule API를 허용합니다.

1. 조직의 관리 계정을 사용하여 https://console.aws.amazon.com/organizations/ AWS Organizations 콘솔을 엽니다.
2. 계정 이름에서 AWS 계정을 선택합니다.

3. 정책 에서 서비스 제어 정책을 확장하고 연결된 SCP 정책을 기록해 둡니다.
4. 페이지 상단에서 정책을 선택합니다.
5. 정책을 선택하고 세부 정보 보기를 선택합니다.
6. JSON 미리 보기 창에서 정책이 DeleteConfigRule API를 허용하는지 확인합니다.

규칙은 서비스 연결 규칙이 아닙니다.

보안 표준을 활성화하면가 서비스 연결 규칙을 AWS Security Hub 생성합니다. 를 사용하여 이러한 서비스 연결 규칙을 삭제할 수 없으며 AWS Config삭제 버튼이 회색으로 표시됩니다. 서비스 연결 규칙을 제거하려면 Security Hub 사용 설명서의 보안 표준 비활성화를 참조하세요.

진행 중인 해결 작업이 없습니다.

문제 해결 작업이 진행 중인 AWS Config 규칙은 삭제할 수 없습니다. 단계에 따라 해당 규칙과 연결된 해결 작업을 삭제합니다. 그런 다음 규칙을 다시 삭제해 보세요.

> **Important**
>
> 실패하거나 성공한 상태의 해결 작업만 삭제합니다.

용 적합성 팩 AWS Config

적합성 팩은 계정 및 리전의 단일 엔터티로 또는의 조직 전체에 쉽게 배포할 수 있는 AWS Config 규칙 및 수정 작업 모음입니다 AWS Organizations.

적합성 팩은 AWS Config 관리형 규칙이나 사용자 지정 규칙 및 문제 해결 작업의 목록이 포함된 YAML 템플릿을 작성하여 만듭니다. AWS Systems Manager 문서(SSM 문서)를 사용하여 적합성 팩 템플릿을에 저장 AWS 하고 SSM 문서 이름을 사용하여 적합성 팩을 직접 배포할 수도 있습니다. AWS Config 콘솔 또는 AWS CLI를 사용하여 템플릿을 배포할 수 있습니다.

빠르게 시작하고 AWS 환경을 평가하려면 샘플 적합성 팩 템플릿 중 하나를 사용합니다. 또한 사용자 지정 적합성 팩을 기반으로 적합성 팩 YAML 파일을 처음부터 작성할 수도 있습니다.

주제

- 에 대한 적합성 팩 대시보드에서 규정 준수 데이터 보기 AWS Config
- 용 적합성 팩의 사전 조건 AWS Config
- 리전 지원
- AWS Config 에 대한 적합성 팩 내 프로세스 검사 AWS Config
- 에 대한 적합성 팩 샘플 템플릿 AWS Config
- 용 사용자 지정 적합성 팩에 대한 템플릿 생성 AWS Config
- 용 적합성 팩 배포 AWS Config
- 에 대한 적합성 팩 편집 AWS Config
- 에 대한 적합성 팩 삭제 AWS Config
- 에 대한 적합성 팩의 세부 정보 및 규정 준수 정보 보기 AWS Config
- 에 대한 적합성 팩의 규정 준수 기록 타임라인 보기 AWS Config
- 에 대한 적합성 팩의 규정 준수 기록 쿼리 AWS Config
- 조직의 모든 계정에서 AWS Config 에 대한 적합성 팩 관리
- 용 적합성 팩 문제 해결 AWS Config

에 대한 적합성 팩 대시보드에서 규정 준수 데이터 보기 AWS Config

적합성 팩의 기본 페이지에는 현재 AWS 계정에서 보유하고 있는 모든 적합성 팩이 표시됩니다. 이 페이지에는 각 적합성 팩의 이름, 배포 상태 및 규정 준수 점수도 포함되어 있습니다. 규정 준수 점수는 적

합성 팩의 가능한 총 규칙-리소스 조합 수와 비교한 적합성 팩의 규정 준수 규칙-리소스 조합 수의 백분율입니다.

이 대시보드를 사용하여 적합성 팩의 규정 준수 수준을 파악하고, 규정 준수 점수를 사용하여 문제 해결 진행 상황을 추적하고, 다양한 요구 사항 세트를 비교하고, 특정 변경 또는 배포가 적합성 팩에 미치는 영향을 확인할 수 있습니다.

적합성 팩 기본 페이지 탐색

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 적합성 팩 페이지로 이동합니다. 적합성 팩 및 해당 규정 준수 점수를 검토합니다. 다음 작업도 수행할 수 있습니다.
   - 새 적합성 팩을 추가하고 구성하려면 적합성 팩 배포를 선택합니다.
   - 적합성 팩 및 해당 데이터를 삭제하거나, 구성 설정을 변경하거나, 전송 위치 또는 파라미터와 같은 추가 세부 정보를 보려면 적합성 팩을 선택하고 작업을 선택합니다.

     > **Note**
     > 배포된 적합성 팩은 편집할 수 없습니다. 적합성 팩의 이름을 선택하고 작업 드롭다운에서 편집을 선택하여 언제든지 다른 선택 항목을 수정할 수 있습니다.

   - 규정 준수 상태 변경 이력을 보려면 적합성 팩을 선택하고 적합성 팩 타임라인을 선택합니다. 자세한 내용은 적합성 팩의 규정 준수 이력 타임라인 보기를 참조하세요.
   - 적합성 팩의 배포 상태, 규정 준수 점수, 규정 준수 점수 타임라인 및 규칙을 자세히 보려면 적합성 팩을 선택하고 보기를 선택합니다.

용 적합성 팩의 사전 조건 AWS Config

적합성 팩을 배포하기 전에 AWS Config 기록을 켭니다.

주제

- 1단계: AWS Config 레코딩 시작(모든 적합성 팩에 필수)
- 2단계: 적합성 팩 유형별 추가 사전 조건

1단계: AWS Config 레코딩 시작(모든 적합성 팩에 필수)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 기록을 시작하려면 기록 꺼짐에서 켜기를 선택합니다. 메시지가 나타나면 계속을 선택합니다.

2단계: 적합성 팩 유형별 추가 사전 조건

A. 문제 해결과 함께 적합성 팩을 사용하기 위한 사전 조건

문제 해결이 포함된 샘플 템플릿을 사용하여 적합성 팩을 배포하기 전에 문제 해결 대상에 따라 자동화 수임 역할 및 기타 리소스와 같은 적절한 AWS 리소스를 생성해야 합니다.

SSM 문서를 사용하여 문제 해결에 사용하는 기존 자동화 역할이 있는 경우 해당 역할의 ARN을 직접 제공할 수 있습니다. 리소스가 있는 경우 템플릿에 해당 리소스를 제공할 수 있습니다.

> **Note**
>
> 문제 해결이 포함된 적합성 팩을 조직에 배포할 때는 조직의 관리 계정 ID를 지정해야 합니다. 그렇지 않으면 조직 적합성 팩을 배포하는 동안 AWS Config 가 자동으로 관리 계정 ID를 멤버 계정 ID로 바꿉니다.

AWS Config 는 자동화 실행 역할 또는에 대한 AWS CloudFormation 내장 함수를 지원하지 않습니다`ConfigRuleName`. 역할의 정확한 ARN을 문자열로 제공해야 하며 내장 함수 없이 전체 규칙 이름을 사용해야 합니다.

정확한 ARN을 전달하는 방법에 대한 자세한 내용은 에 대한 적합성 팩 샘플 템플릿 AWS Config 섹션을 참조하세요. 예제 템플릿을 사용하는 동안 조직의 계정 ID 및 관리 계정 ID를 업데이트합니다.

B. 하나 이상의 사용자 지정 AWS Config 규칙과 함께 적합성 팩을 사용하기 위한 사전 조건

하나 이상의 사용자 지정 AWS Config 규칙이 있는 적합성 팩을 배포하기 전에 AWS Lambda 함수 및 해당 실행 역할과 같은 적절한 리소스를 생성합니다.

기존 사용자 지정 AWS Config 규칙이 있는 경우 AWS Lambda 함수ARN의를 직접 제공하여 해당 사용자 지정 규칙의 다른 인스턴스를 팩의 일부로 생성할 수 있습니다.

기존 사용자 지정 AWS Config 규칙이 없는 경우 AWS Lambda 함수를 생성하고 Lambda 함수의 ARN을 사용할 수 있습니다. 자세한 내용은 AWS Config 사용자 지정 규칙 단원을 참조하십시오.

AWS Lambda 함수가 다른에 있는 경우 적절한 교차 계정 AWS Lambda 함수 권한 부여를 사용하여 AWS Config 규칙을 생성할 AWS 계정수 있습니다. 자세한 내용은 여러 블로그 게시물에서 AWS Config 규칙을 중앙에서 관리하는 방법을 참조하세요 AWS 계정.

Same account bucket policy

가 적합성 팩 아티팩트를 저장할 수 AWS Config 있으려면 Amazon S3 버킷을 제공하고 다음 권한을 추가해야 합니다. 버킷 이름 지정에 대한 자세한 내용은 버킷 이름 지정 규칙을 참조하세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::delivery-bucket-name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::delivery-bucket-name/[optional] prefix/
AWSLogs/AccountId/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
```

```
      }
    }
  ]
}
```

Cross-account bucket policy

가 적합성 팩 아티팩트를 저장할 수 AWS Config 있으려면 Amazon S3 버킷을 제공하고 다음 권한을 추가해야 합니다. 버킷 이름 지정에 대한 자세한 내용은 버킷 이름 지정 규칙을 참조하세요.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms",
            "PutConformancePack API caller user principal like
 arn:aws:iam::SourceAccountId:user/userName "
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
```

```
        }
      }
    },
    {
      "Sid": " AWSConfigConformsBucketReadAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*"
    }
  ]
}
```

> **Note**
>
> 교차 계정 적합성 팩을 배포할 때 전송 Amazon S3 버킷의 이름은 `awsconfigconforms`로 시작해야 합니다.

C. 조직 적합성 팩의 사전 조건

입력 템플릿에 자동 문제 해결 구성이 있는 경우 템플릿에서 문제 해결에 대한 자동화 실행 역할 ARN을 지정합니다. 지정된 이름의 역할이 조직의 모든 계정(관리 및 멤버)에 존재하는지 확인합니다. `PutOrganizationConformancePack`을 호출하기 전에 모든 계정에서 이 역할을 만들어야 합니다. 이 역할을 수동으로 생성하거나 AWS CloudFormation 스택 세트를 사용하여 모든 계정에서이 역할을 생성할 수 있습니다.

템플릿이 AWS CloudFormation 내장 함수`Fn::ImportValue`를 사용하여 특정 변수를 가져오는 경우 해당 변수는 해당 조직의 모든 멤버 계정`Export Value`에서 하나로 정의되어야 합니다.

사용자 지정 AWS Config 규칙은 다중 블로그에서 AWS Config 규칙을 중앙에서 관리하여 적절한 권한을 설정하는 방법을 AWS 계정 참조하세요.

조직 버킷 정책:

가 적합성 팩 아티팩트를 저장할 수 AWS Config 있으려면 Amazon S3 버킷을 제공하고 다음 권한을 추가해야 합니다. 버킷 이름 지정에 대한 자세한 내용은 버킷 이름 지정 규칙을 참조하세요.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                 "s3:GetObject",
                 "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        },
        {
            "Sid": "AllowGetBucketAcl",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        }
    ]
}
```

> **Note**
>
> 조직에 적합성 팩을 배포할 때 전송 Amazon S3 버킷의 이름은 `awsconfigconforms`로 시작해야 합니다.

리전 지원

적합성 팩은 다음 리전에서 지원됩니다.

리전 이름	지역	엔드포인트	프로토콜
미국 동부(오하이오)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
미국 동부(버지니아 북부)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
미국 서부(캘리포니아 북부)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
미국 서부(오레곤)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
아프리카(케이프타운)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
아시아 태평양(홍콩)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
아시아 태평양(하이데라바드)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(자카르타)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
아시아 태평양(멜버른)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
아시아 태평양(뭄바이)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
아시아 태평양(오사카)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
아시아 태평양(서울)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
아시아 태평양(시드니)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
아시아 태평양(도쿄)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
캐나다(중부)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
캐나다 서부(캘거리)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
유럽(프랑크푸르트)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
유럽(아일랜드)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
유럽(런던)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
유럽(밀라노)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
유럽(파리)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
유럽(스페인)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
유럽(스톡홀름)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
유럽(취리히)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
이스라엘(텔아비브)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
중동(바레인)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
중동(UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
남아메리카(상파울루)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 동부)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 서부)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS 조직의 멤버 계정에 적합성 팩을 배포하는 것은 다음 리전에서 지원됩니다.

리전 이름	지역	엔드포인트	프로토콜
미국 동부(오하이오)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
미국 동부(버지니아 북부)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
미국 서부(캘리포니아 북부)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
미국 서부(오레곤)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아프리카(케이프타운)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
아시아 태평양(홍콩)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
아시아 태평양(하이데라바드)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
아시아 태평양(자카르타)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
아시아 태평양(멜버른)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
아시아 태평양(뭄바이)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
아시아 태평양(오사카)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
아시아 태평양(서울)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(시드니)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
아시아 태평양(도쿄)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
캐나다(중부)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
캐나다 서부(캘거리)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
유럽(프랑크푸르트)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
유럽(아일랜드)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
유럽(런던)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
유럽(밀라노)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
유럽(파리)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
유럽(스페인)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
유럽(스톡홀름)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
유럽(취리히)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
이스라엘(텔아비브)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
중동(바레인)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
중동(UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
남아메리카(상파울루)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 동부)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 서부)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config 에 대한 적합성 팩 내 프로세스 검사 AWS Config

프로세스 검사는 적합성 팩의 일부로 확인이 필요한 외부 및 내부 작업을 추적할 수 있는 AWS Config 규칙 유형입니다. 이러한 검사를 기존 적합성 팩이나 새 적합성 팩에 추가할 수 있습니다. 한 곳에서 AWS Config요 및 수동 검사를 포함한 모든 규정 준수를 추적할 수 있습니다.

프로세스 검사를 사용하면 요구 사항 및 작업의 준수 여부를 한 위치에 나열할 수 있습니다. 이러한 프로세스 검사는 규정 준수 체제 기반 적합성 팩의 적용 범위를 확장하는 데 도움이 됩니다. 수동 확인 및 추적이 필요한 프로세스와 작업을 추적하는 새로운 프로세스 검사를 추가하여 규정 준수 팩을 더 확장

할 수 있습니다. 이를 통해 적합성 팩은 규정 준수 체제의 AWS Config요구 사항 및 수동 프로세스에 대한 세부 정보를 제공하는 템플릿이 될 수 있습니다.

적합성 팩 내의 리소스 구성 변경과 관련이 없는 프로세스의 규정 준수를 프로세스 검사로 추적하고 관리할 수 있습니다. 예를 들어, 미디어 백업을 오프사이트 위치에 저장하기 위한 PCI-DSS 규정 준수 요구 사항을 추적하는 프로세스 검사를 추가할 수 있습니다. PCI-DSS 지침 또는 조직의 지침에 따라 이 미디어 백업의 규정 준수 여부를 수동으로 평가하게 됩니다.

리전 가용성: 적합성 팩을 사용한 프로세스 검사는 적합성 팩을 사용할 수 AWS 리전 있는 모든 AWS Config 에서 사용할 수 있습니다. 자세한 내용은 리전 지원 단원을 참조하십시오.

주제

- 프로세스 검사 생성을 위한 샘플 적합성 팩 템플릿
- 적합성 팩에 프로세스 검사를 포함
- 프로세스 검사의 규정 준수 상태 변경
- 프로세스 검사 보기 및 편집(콘솔)

프로세스 검사 생성을 위한 샘플 적합성 팩 템플릿

```
################################################################################
#
#  Conformance Pack template for process check
#
################################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
      Description: Description of Rule
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

다음의 두 가지 샘플 템플릿(CIS AWS 파운데이션 벤치마크 v1.4 레벨 1 운영 모범 사례 템플릿, CIS AWS 파운데이션 벤치마크 v1.4 레벨 2 운영 모범 사례 템플릿)을 참조하세요.

적합성 팩에 프로세스 검사를 포함

1. 적합성 팩 템플릿에 프로세스 검사를 추가합니다. 자세한 내용은 프로세스 검사 생성을 위한 샘플 적합성 팩 템플릿 항목을 참조하세요.

```
Resources:
  ConfigEnabledAllRegions:
    Properties:
      ConfigRuleName: Config-Enabled-All-Regions
      Description: Ensure AWS Config is enabled in all Regions.
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

2. 프로세스 검사의 이름을 입력합니다.
3. 프로세스 검사에 대한 설명을 입력합니다.
4. 적합성 팩 배포 자세한 내용은 용 적합성 팩 배포 AWS Config 섹션을 참조하세요.

프로세스 검사의 규정 준수 상태 변경

AWS Config 콘솔, AWS CLI및 APIs.

Change Compliance Status for Process Checks (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. AWS Config 규칙 페이지로 이동합니다.
3. 템플릿에 지정한 프로세스 검사의 이름을 적합성 팩의 식별자와 함께 선택합니다.

> **Note**
> 동일한 적합성 팩 내의 모든 프로세스 검사에는 동일한 접미사가 붙습니다.

4. 규칙 세부 정보 페이지에서 규칙은 편집할 수 없지만 규칙 준수 여부는 편집할 수 있습니다. 수동 규정 준수 섹션에서 규정 준수 편집을 선택합니다.
5. 드롭다운 목록에서 적절한 규정 준수를 선택합니다.
6. (선택 사항) 규정 준수 상태에 대한 설명을 입력합니다.

7. 저장을 선택합니다.

Change the Compliance Status for Process Checks (AWS CLI)

AWS Command Line Interface ()를 사용하여 적합성 팩 내에서 프로세스 검사의 규정 준수를 업데이트할 수 있습니다AWS CLI.

로컬 시스템에 AWS CLI 를 설치하려면 AWS CLI 사용 설명서의 설치를 AWS CLI 참조하세요.

필요한 경우 적합성 팩을 사용할 수 있는 리전 AWS CLI 을 사용하도록를 구성`AWS Configure`하려면 AWS Config 를 AWS 입력합니다.

1. 명령 프롬프트 또는 터미널 창을 엽니다.
2. 다음 명령을 입력하여 `ComplianceResourceId`이 `Account ID`인 프로세스 규정 준수를 업데이트하고 규칙 이름을 포함합니다.

```
aws configservice put-external-evaluation --config-rule-
name process-check-rule-name  --external-evaluation
 ComplianceResourceType=AWS::::Account,ComplianceResourceId=Account
 ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. 입력을 눌러 명령을 실행합니다.

Change the Compliance Status for Process Checks (API)

배포가 완료된 후 `PutExternalEvaluation` API를 사용하여 프로세스 검사의 평가 및 규정 준수를 업데이트합니다. 자세한 내용은 PutExternalEvaluation를 참조하세요.

프로세스 검사 보기 및 편집(콘솔)

프로세스 검사에 규정 준수 상태가 추가되어 있어야만 프로세스 검사를 볼 수 있습니다. 특정 적합성 팩을 선택하면 해당 준수 팩 내의 모든 프로세스 검사를 볼 수 있습니다. 여기에서 준수 및 비준수 상태인 프로세스 검사 목록을 볼 수 있습니다.

서비스 연결 규칙이므로 규칙 세부 정보 페이지를 통해 프로세스 검사를 편집할 수 없습니다.

> **Note**
> 하지만 규정 준수 편집을 선택하고 규정 준수, 규정 미준수 또는 해당 사항 없음 중에서 적절한 값을 선택하여 프로세스 검사의 규정 준수 여부를 업데이트할 수 있습니다.

프로세스 검사를 추가한 적합성 팩에서 프로세스 검사를 편집하거나 삭제할 수 있습니다.

에 대한 적합성 팩 샘플 템플릿 AWS Config

다음은 AWS Config 콘솔에 표시되는 적합성 팩 YAML 템플릿입니다. 각 적합성 팩 템플릿 내에서 하나 이상의 AWS Config 규칙 및 문제 해결 작업을 사용할 수 있습니다. 적합성 팩에 나열된 규칙은 AWS Config AWS Config 관리형 규칙 및/또는 AWS Config 사용자 지정 규칙일 수 있습니다. 모든 적합성 팩 템플릿은 GitHub에서 다운로드할 수 있습니다.

> **Important**
> 적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성하는 데 도움이 되는 범용 규정 준수 프레임워크를 제공합니다. AWS 적합성 팩 샘플 템플릿은 환경에 적합한 다른 규칙 또는 추가 규칙, 입력 파라미터 및 문제 해결 작업을 사용하여 자체 적합성 팩을 생성하는 데 도움이 되도록 설계되었습니다. 규정 준수 표준 및 업계 벤치마크와 관련된 템플릿을 포함한 샘플 템플릿은 특정 거버넌스 표준을 준수하도록 설계되지 않았습니다. 내부 작업을 대체하거나 규정 준수 평가를 통과하도록 보장할 수 없습니다.

> **Note**
> 적합성 팩을 배포하는 리전에서 사용할 수 있는 규칙(리전 가용성별 AWS Config 관리형 규칙 목록)을 검토하고 배포하기 전에 해당 리전에서 아직 사용할 수 없는 규칙에 대한 템플릿을 수정하는 것이 좋습니다.

주제

- AWS Control Tower Detective Guardrails 적합성 팩
- ABS CCIG 2.0 중요 워크로드 운영 모범 사례

- ABS CCIG 2.0 표준 워크로드 운영 모범 사례
- ACSC Essential 8 운영 모범 사례
- ACSC ISM 운영 모범 사례
- AI 및 ML 운영 모범 사례
- Amazon API Gateway 운영 모범 사례
- Amazon CloudWatch 운영 모범 사례
- Amazon DynamoDB 운영 모범 사례
- Amazon S3 운영 모범 사례
- APRA CPG 234 운영 모범 사례
- 자산 관리 운영 모범 사례
- AWS Backup운영 모범 사례
- AWS 자격 증명 및 액세스 관리를 위한 운영 모범 사례
- AWS Well-Architected Framework 신뢰성 원칙의 운영 모범 사례
- AWS Well-Architected Framework 보안 원칙의 운영 모범 사례
- BCP 및 DR 운영 모범 사례
- BNM RMiT 운영 모범 사례
- 캐나다 사이버 보안 센터(CCCS) 중간 클라우드 제어 프로필 운영 모범 사례
- CIS AWS 파운데이션 벤치마크 v1.4 레벨 1 운영 모범 사례
- CIS AWS 파운데이션 벤치마크 v1.4 레벨 2 운영 모범 사례
- CIS Critical Security Controls v8 IG1 운영 모범 사례
- CIS 핵심 보안 제어 v8 IG2 운영 모범 사례
- CIS 핵심 보안 제어 v8 IG3 운영 모범 사례
- CIS 운영 모범 사례 상위 20개
- CISA Cyber Essentials의 운영 모범 사례
- 미국 연방수사국 형사사법정보부(CJIS) 운영 모범 사례
- CMMC 2.0 레벨 1 운영 모범 사례
- CMMC 2.0 레벨 2 운영 모범 사례
- 컴퓨팅 서비스 운영 모범 사례

- 데이터 복원력 운영 모범 사례
- 데이터베이스 서비스 운영 모범 사례
- 데이터 레이크 및 분석 서비스 운영 모범 사례
- DevOps 운영 모범 사례
- EC2 운영 모범 사례
- 암호화 및 키 관리 운영 모범 사례
- SME를 위한 ENISA 사이버 보안 가이드 운영 모범 사례
- Esquema Nacional de Seguridad(ENS) Low 운영 모범 사례
- Esquema Nacional de Seguridad(ENS) Medium 운영 모범 사례
- Esquema Nacional de Seguridad(ENS) High 운영 모범 사례
- FDA 타이틀 21 CFR 파트 11 운영 모범 사례
- FedRAMP(Low) 운영 모범 사례
- FedRAMP(Moderate) 운영 모범 사례
- FedRAMP(High 파트 1) 운영 모범 사례
- FedRAMP(High 파트 2) 운영 모범 사례
- FFIEC 운영 모범 사례
- 독일 C5(Cloud Computing Compliance Criteria Catalog) 운영 모범 사례
- Gramm Leach Bliley 법(GLBA) 운영 모범 사례
- GxP EU Annex 11 운영 모범 사례
- HIPAA 보안 운영 모범 사례
- IRS 1075 운영 모범 사례
- K-ISMS 운영 모범 사례
- 로드 밸런싱 운영 모범 사례
- 로깅 운영 모범 사례
- 관리 및 거버넌스 서비스 운영 모범 사례
- MAS Notice 655 운영 모범 사례
- MAS TRMG 운영 모범 사례
- 모니터링 운영 모범 사례

- NBC TRMG 운영 모범 사례
- NERC CIP BCSI 운영 모범 사례
- NCSC 클라우드 보안 원칙 운영 모범 사례
- NCSC 사이버 평가 프레임워크 운영 모범 사례
- 네트워킹 및 콘텐츠 전송 서비스 운영 모범 사례
- NIST 800-53 rev 4 운영 모범 사례
- NIST 800-53 rev 5 운영 모범 사례
- NIST 800 171 운영 모범 사례
- NIST 800 172 운영 모범 사례
- NIST 800 181 운영 모범 사례
- NIST 1800 25 운영 모범 사례
- NIST CSF 운영 모범 사례
- NIST 개인정보보호 프레임워크 v1.0 운영 모범 사례
- NYDFS 23 운영 모범 사례
- NZISM 3.8 운영 모범 사례
- PCI DSS 3.2.1 운영 모범 사례
- PCI DSS 4.0 운영 모범 사례(글로벌 리소스 유형 제외)
- PCI DSS 4.0 운영 모범 사례(글로벌 리소스 유형 포함)
- 공개적으로 액세스 가능한 리소스 운영 모범 사례
- UCB용 RBI 사이버 보안 프레임워크 운영 모범 사례
- RBI MD-ITF 운영 모범 사례
- 보안, 자격 증명 및 규정 준수 서비스 운영 모범 사례
- 서버리스 운영 모범 사례
- 스토리지 서비스 운영 모범 사례
- SWIFT CSP 운영 모범 사례
- Amazon Elastic Container Service(Amazon ECS) 보안 모범 사례
- Amazon Elastic File System(Amazon EFS) 보안 모범 사례
- Amazon Elastic Kubernetes Service(Amazon EKS) 보안 모범 사례
- Amazon CloudFront 보안 모범 사례

- Amazon OpenSearch Service 보안 모범 사례
- Amazon Redshift 보안 모범 사례
- Amazon Relational Database Service(RDS) 보안 모범 사례
- AWS Auto Scaling보안 모범 사례
- AWS CloudTrail보안 모범 사례
- AWS CodeBuild보안 모범 사례
- Amazon ECR 보안 모범 사례
- AWS Lambda보안 모범 사례
- AWS Network Firewall보안 모범 사례
- Amazon SageMaker AI의 보안 모범 사례
- AWS Secrets Manager보안 모범 사례
- AWS WAF보안 모범 사례
- 문제 해결 작업이 포함된 템플릿의 예

AWS Control Tower Detective Guardrails 적합성 팩

이 적합성 팩에는 AWS Control Tower Detective 가드레일을 기반으로 하는 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub의 AWS Control Tower 탐지 가드레일 규정 준수 팩에서 제공됩니다.

ABS CCIG 2.0 중요 워크로드 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 ABS 클라우드 컴퓨팅 구현 가이드 2.0 - 재료 워크로드와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 ABS 클라우드 컴퓨

팅 구현 가이드 제어와 관련이 있습니다. 한 ABS 클라우드 컴퓨팅 구현 가이드 제어가 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-2-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
section4a-govern-the-cloud-2-material-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구

제어 ID	AWS 구성 규칙	지침
		성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-3-material-workloads	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4a-govern-the-cloud-3-material-workloads	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-3-standard-workloads	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-material-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
section4b-design-and-secure-the-cloud-3-material-workloads	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
section4b-design-and-secure-the-cloud-3-material-workloads	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-material-workloads	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
section4b-design-and-secure-the-cloud-3-material-workloads	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-material-workloads	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
section4b-design-and-secure-the-cloud-3-material-workloads	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-material-workloads	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.
section4b-design-and-secure-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
section4b-design-and-secure-the-cloud-4-material-workloads	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-material-workloads	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-4-material-workloads	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-material-workloads	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
section4b-design-and-secure-the-cloud-4-material-workloads	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-material-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
section4b-design-and-secure-the-cloud-4-material-workloads	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-4-material-workloads	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-material-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-4-material-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-material-workloads	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
section4b-design-and-secure-the-cloud-4-material-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-material-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
section4b-design-and-secure-the-cloud-5-material-workloads	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.
section4b-design-and-secure-the-cloud-5-material-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-5-material-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
section4b-design-and-secure-the-cloud-5-material-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-5-material-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
section4b-design-and-secure-the-cloud-6-material-workloads	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.
section4b-design-and-secure-the-cloud-6-material-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-material-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-6-material-workloads	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-8-material-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-8-material-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-material-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail 에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-9-material-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail 에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
section4b-design-and-secure-the-cloud-9-material-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-9-material-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-material-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
section4b-design-and-secure-the-cloud-10-material-workloads	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
section4b-design-and-secure-the-cloud-10-material-workloads	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-10-material-workloads	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-10-material-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
section4b-design-and-secure-the-cloud-10-material-workloads	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
section4b-design-and-secure-the-cloud-10-material-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
section4b-design-and-secure-the-cloud-10-material-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
section4b-design-and-secure-the-cloud-10-material-workloads	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-10-material-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
section4b-design-and-secure-the-cloud-10-material-workloads	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-material-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-10-material-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서로 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
section4b-design-and-secure-the-cloud-11-material-workloads	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
section4b-design-and-secure-the-cloud-11-material-workloads	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-11-material-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
section4b-design-and-secure-the-cloud-11-material-workloads	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
section4b-design-and-secure-the-cloud-11-material-workloads	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-11-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
section4b-design-and-secure-the-cloud-11-material-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-11-material-workloads	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
section4b-design-and-secure-the-cloud-11-material-workloads	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-11-material-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
section4b-design-and-secure-the-cloud-11-material-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-11-material-workloads	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
section4b-design-and-secure-the-cloud-11-material-workloads	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 보안 인증 정보가 포함되지 않도록 합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-material-workloads	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
section4b-design-and-secure-the-cloud-14-material-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
section4b-design-and-secure-the-cloud-14-material-workloads	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-material-workloads	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
section4b-design-and-secure-the-cloud-14-material-workloads	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
section4b-design-and-secure-the-cloud-14-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-material-workloads	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
section4b-design-and-secure-the-cloud-14-material-workloads	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-material-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail 에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
section4b-design-and-secure-the-cloud-15-material-workloads	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
section4b-design-and-secure-the-cloud-15-material-workloads	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-material-workloads	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
section4b-design-and-secure-the-cloud-15-material-workloads	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
section4c-run-the-cloud-2-material-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-2-material-workloads	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 유지할 기회를 줄이는 데 도움이 됩니다.
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되도록 합니다.
section4c-run-the-cloud-4-material-workloads	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
section4c-run-the-cloud-4-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-4-material-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-6-material-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
section4c-run-the-cloud-6-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
section4c-run-the-cloud-6-material-workloads	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

템플릿

이 템플릿은 GitHub: Operational Best Practices for ABS CCIG 2.0 Material Workloads에서 사용할 수 있습니다.

ABS CCIG 2.0 표준 워크로드 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 ABS 클라우드 컴퓨팅 구현 가이드 2.0 - 표준 워크로드와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 ABS 클라우드 컴퓨팅 구현 가이드 제어와 관련이 있습니다. 한 ABS 클라우드 컴퓨팅 구현 가이드 제어가 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail 에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전

제어 ID	AWS 구성 규칙	지침
		에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.
section4a-govern-the-cloud-3-standard-workloads	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail 에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Kinesis Streams에 암호화를 활성화해야 합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Kinesis Streams에 암호화를 활성화해야 합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail의 사용이 포함됩니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서로 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 보안 인증 정보가 포함되지 않도록 합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Kinesis Streams에 암호화를 활성화해야 합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 유지할 기회를 줄이는 데 도움이 됩니다.
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
section4c-run-the-cloud-3-standard-workloads	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
section4c-run-the-cloud-3-standard-workloads	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되도록 합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	AWS 구성 규칙	지침
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

템플릿

이 템플릿은 GitHub: Operational Best Practices for ABS CCIG 2.0 Standard Workloads에서 사용할 수 있습니다.

ACSC Essential 8 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 호주 사이버 보안 센터(ACSC) Essential Eight 성숙도 모델과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 ACSC Essential Eight 제어와 관련이 있습니다. 한 ACSC Essential Eight 제어가 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요. Config 규칙에 대한 매핑 중 일부는 다른 보다 규범적인 섹션에 비해 고차원적인 섹션입니다(예: 사이버 보안 인시던트의 범위를 제한하기 위한 완화 전략).

이 샘플 적합성 팩 템플릿에는 호주 연방에서 작성한 ACSC Essential 8 내의 제어에 대한 매핑이 포함되어 있으며 해당 제어는 ACSC | Essential Eight에서 확인할 수 있습니다. Creative Commons 권한 4.0 국제 공개 라이선스에 따른 프레임워크 라이선싱 및 프레임워크 저작권 정보(보증 면책 조항 포함)는 ACSC | Copyright에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Application_control	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.
Application_control	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청

제어 ID	AWS 구성 규칙	지침
		을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
Application_control	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
Application_control	waf-regional-rule-not-empty	AWS WAF에 비어 있지 않은 규칙이 있는지 확인합니다. 조건이 없는 규칙에는 의도하지 않은 동작이 발생할 수 있습니다.
Application_control	waf-regional-rulegroup-not-empty	AWS WAF에 비어 있지 않은 규칙 그룹이 있는지 확인합니다. 규칙 그룹이 비어 있으면 의도하지 않은 동작이 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Application_control	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.
Application_control	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
Patch_applications	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Patch_applications	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
Patch_applications	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. Fargate 플랫폼 버전에 AWS 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.

제어 ID	AWS 구성 규칙	지침
Patch_applications	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
Patch_applications	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
Patch_applications	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
Patch_applications	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
Restrict_administrative_privileges	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
Restrict_administrative_privileges	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Restrict_administrative_privileges	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
Restrict_administrative_privileges	codebuild-project-environment-privileged-check	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있지 않은지 확인합니다. Docker API와 컨테이너의 기본 하드웨어에 대해 의도하지 않은 액세스를 방지하려면 이 설정을 비활성화해야 합니다.

제어 ID	AWS 구성 규칙	지침
Restrict_administrative_privileges	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).
Restrict_administrative_privileges	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
Restrict_administrative_privileges	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Restrict_administrative_privileges	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.
Restrict_administrative_privileges	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Restrict_administrative_privileges	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
Restrict_administrative_privileges	rds-instance-iam-authentication-enabled	시스템 및 자산에 대한 액세스를 제어하기 위해 Amazon Relational Database Service(Amazon RDS) 인스턴스에서 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. 이렇게 하면 데이터베이스를 오가는 네트워크 트래픽이 SSL(Secure Sockets Layer)을 통해 암호화됩니다. 인증은 외부에서 관리되므로 사용자 보안 인증 정보를 데이터베이스에 저장할 필요가 없습니다.

제어 ID	AWS 구성 규칙	지침
Restrict_administrative_privileges	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
Restrict_administrative_privileges	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
Restrict_administrative_privileges	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Restrict_administrative_privileges	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
Restrict_administrative_privileges	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Patch_operating_systems	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager 에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	AWS 구성 규칙	지침
Multi-factor_authentication	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
Multi-factor_authentication	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
Multi-factor_authentication	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
Multi-factor_authentication	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
Multi-factor_authentication	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
Regular_backups	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
Regular_backups	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Regular_backups	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Regular_backups	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Regular_backups	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Regular_backups	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Regular_backups	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
Regular_backups	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Regular_backups	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Regular_backups	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Regular_backups	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
Regular_backups	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.
Regular_backups	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

템플릿

이 템플릿은 GitHub: Operational Best Practices for ACSC Essential 8에서 사용할 수 있습니다.

ACSC ISM 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 호주 사이버 보안 센터(ACSC) 정보 보안 매뉴얼(ISM) 2020년 6월과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 ISM 제어와 관련이 있습니다. 한 ISM 제어가 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 샘플 적합성 팩 템플릿에는 호주 연방에서 작성한 ISM 프레임워크 내의 제어에 대한 매핑이 포함되어 있으며 해당 제어는 Australian Government Information Security Manual에서 확인할 수 있습니다. Creative Commons 권한 4.0 국제 공개 라이선스에 따른 프레임워크 라이선싱 및 프레임워크 저작권 정보(보증 면책 조항 포함)는 ACSC | Copyright에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
43	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되도록 합니다.
252	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.
261	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를

제어 ID	AWS 구성 규칙	지침
		통해 사용자 활동을 파악할 수 있습니다.
261	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
261	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	AWS 구성 규칙	지침
298	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
298	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
298	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
298	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
380	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	AWS 구성 규칙	지침
459	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
459	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
459	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
459	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
459	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
459	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
459	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
459	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
459	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
459	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
459	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
459	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
459	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
459	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
459	codebuild-project-s3-logs-encrypted	저장 시 민감한 데이터를 보호하려면 Amazon S3에 저장된 your AWS CodeBuild 로그에 대해 암호화가 활성화되어 있는지 확인하세요.
459	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
459	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Kinesis Streams에 암호화를 활성화해야 합니다.
459	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
459	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
459	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
580	audit-log-policy-exists(프로세스 확인)	조직의 로깅 요구 사항을 정의하는 감사 로그 관리 정책을 수립하고 유지 관리합니다. 여기에는 감사 로그의 검토 및 보존이 포함되며 이에 국한되지는 않습니다.

제어 ID	AWS 구성 규칙	지침
634	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
859	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
974	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
974	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
1139	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
1173	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
1173	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
1173	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
1173	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
1173	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1228	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
1240	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.
1240	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
1271	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1271	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.
1277	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
1277	rds-instance-iam-authentication-enabled	시스템 및 자산에 대한 액세스를 제어하기 위해 Amazon Relational Database Service(Amazon RDS) 인스턴스에서 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. 이렇게 하면 데이터베이스를 오가는 네트워크 트래픽이 SSL(Secure Sockets Layer)을 통해 암호화됩니다. 인증은 외부에서 관리되므로 사용자 보안 인증 정보를 데이터베이스에 저장할 필요가 없습니다.
1277	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
1380	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1380	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
1380	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. Fargate 플랫폼 버전에 AWS 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.

제어 ID	AWS 구성 규칙	지침
1380	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
1380	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
1380	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
1380	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
1380	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
1380	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
1380	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
1380	codebuild-project-environment-privileged-check	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있지 않은지 확인합니다. Docker API와 컨테이너의 기본 하드웨어에 대해 의도하지 않은 액세스를 방지하려면 이 설정을 비활성화해야 합니다.

제어 ID	AWS 구성 규칙	지침
1380	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).
1380	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
1380	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
1380	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.
1380	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1380	rds-instance-iam-authentication-enabled	시스템 및 자산에 대한 액세스를 제어하기 위해 Amazon Relational Database Service(Amazon RDS) 인스턴스에서 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. 이렇게 하면 데이터베이스를 오가는 네트워크 트래픽이 SSL(Secure Sockets Layer)을 통해 암호화됩니다. 인증은 외부에서 관리되므로 사용자 보안 인증 정보를 데이터베이스에 저장할 필요가 없습니다.
1380	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
1380	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	AWS 구성 규칙	지침
1380	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
1380	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
1380	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1388	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
1388	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1401	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
1401	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
1401	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
1401	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
1401	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
1402	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
1404	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
1405	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
1405	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1405	multi-region-cloudtrail-enabled	MULTI_REGION_CLOUD_TRAIL_ENABLED
1405	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
1405	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
1405	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1405	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
1405	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
1405	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
1405	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
1405	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
1405	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
1405	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
1405	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	AWS 구성 규칙	지침
1405	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.
1405	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
1405	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1490	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.
1490	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
1490	waf-regional-rule-not-empty	AWS WAF에 비어 있지 않은 규칙이 있는지 확인합니다. 조건이 없는 규칙에는 의도하지 않은 동작이 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1490	waf-regional-rulegroup-not-empty	AWS WAF에 비어 있지 않은 규칙 그룹이 있는지 확인합니다. 규칙 그룹이 비어 있으면 의도하지 않은 동작이 발생할 수 있습니다.
1490	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.
1490	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
1501	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	AWS 구성 규칙	지침
1504	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
1504	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
1504	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
1504	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
1504	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
1509	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
1509	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1509	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
1509	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
1509	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
1509	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
1509	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
1509	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1509	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
1509	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
1509	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
1509	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
1509	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
1509	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
1509	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.
1509	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
1509	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1511	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
1511	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
1511	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	AWS 구성 규칙	지침
1511	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
1511	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
1511	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1511	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
1511	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
1511	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
1511	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1511	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
1511	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.
1511	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1511	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.
1511	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
1511	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.
1511	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1515	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
1515	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
1515	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1515	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
1515	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
1515	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1515	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
1515	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
1515	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1515	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.
1515	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1515	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
1515	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
1536	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
1537	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
1537	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
1552	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
1552	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1552	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	AWS 구성 규칙	지침
1552	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1552	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
1579	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1580	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
1580	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1580	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
1650	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
1650	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1650	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
1650	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail의 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
1650	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
1650	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
1650	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
1650	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1650	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
1650	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
1650	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
1650	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
1650	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
1650	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
1650	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.
1650	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
1650	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1657	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.
1657	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
1657	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
1657	waf-regional-rule-not-empty	AWS WAF에 비어 있지 않은 규칙이 있는지 확인합니다. 조건이 없는 규칙에는 의도하지 않은 동작이 발생할 수 있습니다.
1657	waf-regional-rulegroup-not-empty	AWS WAF에 비어 있지 않은 규칙 그룹이 있는지 확인합니다. 규칙 그룹이 비어 있으면 의도하지 않은 동작이 발생할 수 있습니다.
1657	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.

제어 ID	AWS 구성 규칙	지침
1657	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
1661	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
1661	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1661	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
1661	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
1661	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
1661	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
1661	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
1661	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1661	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
1661	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
1661	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
1661	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
1661	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
1661	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
1679	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
1679	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
1679	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
1679	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
1679	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
1680	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
1680	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
1680	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
1680	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
1680	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
1681	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
1681	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
1681	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
1681	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
1681	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
1683	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1683	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
1690	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1690	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
1690	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. Fargate 플랫폼 버전에 AWS 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.

제어 ID	AWS 구성 규칙	지침
1690	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
1690	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
1690	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
1690	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
1691	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1691	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
1691	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. Fargate 플랫폼 버전에 AWS 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.

제어 ID	AWS 구성 규칙	지침
1691	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
1691	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
1691	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
1691	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
1693	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1693	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
1693	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. Fargate 플랫폼 버전에 AWS 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.

제어 ID	AWS 구성 규칙	지침
1693	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
1693	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
1693	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
1693	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
1694	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	AWS 구성 규칙	지침
1695	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager 에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
1707	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
P1	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
P1	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
P3	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
P5	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
P7	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
P7	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
P7	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
P7	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
P8	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
P9	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
P9	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.
P9	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
P9	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
P9	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.
P9	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
P9	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
P9	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
P9	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
P9	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
P9	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
P9	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
P9	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
P9	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	AWS 구성 규칙	지침
P10	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
P10	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
P10	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
P10	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
P10	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
P11	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

템플릿

이 템플릿은 GitHub: Operational Best Practices for ACSC ISM에서 사용할 수 있습니다.

AI 및 ML 운영 모범 사례

이 적합성 팩에는 AI 및 ML 기반 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

이 템플릿은 GitHub: Operational Best Practices for AI and ML에서 사용할 수 있습니다.

Amazon API Gateway 운영 모범 사례

이 적합성 팩에는 내 Amazon API Gateway 사용량에 따른 AWS Config 규칙이 포함되어 있습니다 AWS. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

이 템플릿은 GitHub: Operational Best Practices for Amazon API Gateway에서 사용할 수 있습니다.

Amazon CloudWatch 운영 모범 사례

이 적합성 팩에는 Amazon CloudWatch의 사용량에 따른 AWS Config 규칙이 포함되어 있습니다 AWS. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

이 템플릿은 GitHub: Operational Best Practices for Amazon CloudWatch에서 사용할 수 있습니다.

Amazon DynamoDB 운영 모범 사례

이 템플릿은 GitHub: Operational Best Practices for Amazon DynamoDB에서 사용할 수 있습니다.

Amazon S3 운영 모범 사례

이 템플릿은 GitHub: Operational Best Practices for Amazon S3에서 사용할 수 있습니다.

APRA CPG 234 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 호주 건전성 규제 기관(APRA) CPG 234와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 APRA CPG 234 제어와 관련이 있습니다. 한 APRA CPG 234 제어가 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 샘플 적합성 팩 템플릿에는 호주 연방에서 작성한 APRA CPG 234 2019 내의 제어에 대한 매핑이 포함되어 있으며 해당 제어는 Prudential Practice Guide: CPG 234 Information Security에서 확인할 수 있습니다. Creative Commons 권한 3.0 호주 라이선스에 따른 프레임워크 라이선싱 및 프레임워크 저작권 정보(보증 면책 조항 포함)는 APRA | Copyright에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36a	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic

제어 ID	AWS 구성 규칙	지침
		Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
36a	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
36a	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	AWS 구성 규칙	지침
36b	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
36b	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
36b	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager 에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
36b	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail 에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
36b	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
36b	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	AWS 구성 규칙	지침
36b	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
36c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
36c	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36c	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
36c	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
36c	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
36c	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
36c	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36c	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
36c	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
36d	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36d	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
36d	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36d	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
36d	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
36d	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
36d	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36d	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
36d	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	AWS 구성 규칙	지침
36d	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36d	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36d	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
36d	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
36d	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
36d	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36d	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
36d	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
36d	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
36d	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
36d	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
36d	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36d	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
36d	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
36d	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
36d	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
36d	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
36d	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
36d	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
36d	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
36d	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
36d	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
36d	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
36d	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36d	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
36d	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
36d	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
36d	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
36d	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
36d	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	AWS 구성 규칙	지침
36d	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
36d	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36d	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
36e	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
36e	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36e	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36e	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36e	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
36e	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
36e	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
36e	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
36e	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36e	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
36e	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	AWS 구성 규칙	지침
36e	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36e	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36e	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
36e	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
36e	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
36e	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
36e	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36e	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
36e	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
36e	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	AWS 구성 규칙	지침
36e	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
36e	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.
36e	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
36e	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
36e	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36e	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
36f	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36f	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
36f	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36f	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
36f	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
36f	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
36f	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36f	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
36f	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	AWS 구성 규칙	지침
36f	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36f	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
36f	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
36f	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
36f	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
36f	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36f	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
36f	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
36f	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
36f	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36f	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.
36f	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
36f	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
36f	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
36f	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
36f	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	AWS 구성 규칙	지침
36f	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
36f	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
36f	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
36f	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
36g	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
36g	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
36g	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
36h	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
36h	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
36h	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36h	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
36h	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
36h	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
36h	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
36h	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
36i	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	AWS 구성 규칙	지침
36i	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
36i	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
36i	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
36i	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.
36i	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.
36i	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	AWS 구성 규칙	지침
36i	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
36i	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
36i	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
36i	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36j	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
36j	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
36j	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
36j	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36j	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
36j	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
36j	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
36j	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
36j	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.
36j	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	AWS 구성 규칙	지침
36j	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
36l	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
36l	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36I	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
36I	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
36I	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36l	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36l	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
36l	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
36l	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
36l	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36l	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
36l	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
36l	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
36l	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
36l	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
36l	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	AWS 구성 규칙	지침
36l	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
39(a)(b)(d)	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
39(a)(b)(d)	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
39(a)(b)(d)	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
40	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
40	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
40	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
40	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
44a	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
44a	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
44a	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
44b	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
44b	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
44b	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
44c	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	AWS 구성 규칙	지침
44c	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
44c	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEnc ryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
44c	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
45	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
45	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
45	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
45	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
45	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
45	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
45	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
45	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
45	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
45	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
45	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
45	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
45	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
45	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
45	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
45	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
45	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
45	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	AWS 구성 규칙	지침
45	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
45	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
45	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
45	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
45	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
45	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
45	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
45	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
45	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
45	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
45	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
45	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
45	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
45	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
45	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
45	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
45	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
45	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
45	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
45	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	AWS 구성 규칙	지침
45	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
45	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	AWS 구성 규칙	지침
45	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
45	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
45	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
47c	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.
47c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
47c	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
47c	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
47c	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
47c	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
47c	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
52c	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
52c	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
52c	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.
52c	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
52c	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
52c	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
52c	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
52c	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
52c	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
52c	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
52c	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
52c	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
52c	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
52c	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	AWS 구성 규칙	지침
52c	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
52c	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
52c	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
52c	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
52d	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
52d	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
52d	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
52d	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
52d	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
52d	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
52d	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
52d	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
52d	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	AWS 구성 규칙	지침
52d	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
52d	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
52d	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
52d	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
52d	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
52d	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
52d	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
52d	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
52d	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
52d	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	AWS 구성 규칙	지침
52d	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
52d	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
52d	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
52d	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
52e	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
52e	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
53	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
53	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
53	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
53	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
53	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
53	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
53	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
53	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
53	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
53	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
53	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
53	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
53	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	AWS 구성 규칙	지침
53	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
53	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
53	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
53	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
53	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
53	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	AWS 구성 규칙	지침
53	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
53	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	AWS 구성 규칙	지침
53	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
53	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
54	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
54	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
54	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
54	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
54	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
54	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.
54	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
54	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
54	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	AWS 구성 규칙	지침
54	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
54	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
54	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
54	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
54	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
54	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
54	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
54	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
54	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
54	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
54	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
54	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
54	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
54	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
54	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
54	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
54	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
55	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
55	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
67	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
67	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
67	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
67	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
67	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
67	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
67	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
67	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
67	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
67	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	AWS 구성 규칙	지침
67	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
67	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
67	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
67	opensearch-logs-to-cloudwat ch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
67	ec2-managedinstance-patch-c ompliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Ama zon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager 에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	AWS 구성 규칙	지침
67	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
67	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
67	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
68	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
68	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
73	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
73	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(b)(h)	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.
AttachmentA_1(b)(h)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(b)(h)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
AttachmentA_1(b)(h)	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(b)(h)	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AttachmentA_1(b)(h)	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(b)(h)	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(b)(h)	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
AttachmentA_1(b)(h)	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AttachmentA_1(b)(h)	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(c)	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
AttachmentA_1(c)	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(e)	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
AttachmentA_1(e)	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(e)	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
AttachmentA_1(e)	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AttachmentA_1(e)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(e)	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AttachmentA_1(e)	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
AttachmentA_1(e)	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(e)	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
AttachmentA_1(e)	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(e)	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
AttachmentA_1(e)	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AttachmentA_1(e)	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	AWS 구성 규칙	지침
AttachmentA_1(e)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AttachmentA_1(e)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AttachmentB_1	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_4	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_4	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_4	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AttachmentC_4	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
AttachmentC_4	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_4	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
AttachmentC_4	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AttachmentC_4	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_4	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AttachmentC_4	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
AttachmentC_4	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AttachmentC_4	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
AttachmentC_4	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_4	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AttachmentC_4	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_4	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
AttachmentC_4	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
AttachmentC_4	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_5	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AttachmentC_5	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
AttachmentC_5	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AttachmentC_5	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_5	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_6	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AttachmentC_6	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AttachmentC_6	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_7(c)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
AttachmentC_7(h)	api-gw-execution-logging-en abled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AttachmentC_7(h)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
AttachmentC_7(h)	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AttachmentC_7(h)	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_7(h)	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
AttachmentC_7(h)	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_7(h)	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AttachmentC_7(h)	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_7(h)	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AttachmentC_7(h)	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_7(h)	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
AttachmentC_7(h)	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AttachmentC_7(h)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_7(h)	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
AttachmentC_7(h)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_7(i)	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AttachmentC_7(j)	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_7(j)	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AttachmentC_7(j)	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
AttachmentC_7(j)	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AttachmentC_8	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AttachmentC_8	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AttachmentC_8	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
AttachmentC_8	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AttachmentC_8	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
AttachmentC_8	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_8	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
AttachmentC_8	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_8	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
AttachmentC_8	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AttachmentC_8	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentC_8	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AttachmentD_1	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
AttachmentD_1	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 보안 인증 정보가 포함되지 않도록 합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentE_4	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
AttachmentE_4	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.
AttachmentE_5(d)	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.
AttachmentE_1(a)(b)(d)	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentE_1(a)(b)(d)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AttachmentE_1(a)(b)(d)	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
AttachmentE_1(a)(b)(d)	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentE_1(a)(b)(d)	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
AttachmentE_1(a)(b)(d)	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
AttachmentE_1(a)(b)(d)	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.
AttachmentE_1(a)(b)(d)	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
AttachmentE_1(a)(b)(d)	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentE_1(a)(b)(d)	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
AttachmentE_1(a)(b)(d)	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
AttachmentE_1(a)(b)(d)	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	AWS 구성 규칙	지침
AttachmentE_1(a)(b)(d)	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
AttachmentE_1(a)(b)(d)	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
AttachmentE_1(a)(b)(d)	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentE_1(a)(b)(d)	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
AttachmentE_1(a)(b)(d)	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AttachmentE_1(a)(b)(d)	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentE_1(a)(b)(d)	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AttachmentE_1(a)(b)(d)	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AttachmentE_1(a)(b)(d)	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentE_1(a)(b)(d)	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
AttachmentE_1(a)(b)(d)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AttachmentE_1(a)(b)(d)	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
AttachmentE_1(a)(b)(d)	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AttachmentE_1(a)(b)(d)	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

템플릿

이 템플릿은 GitHub: Operational Best Practices for APRA CPG 234에서 사용할 수 있습니다.

자산 관리 운영 모범 사례

이 적합성 팩에는 내 자산 관리를 기반으로 하는 AWS Config 규칙이 포함되어 있습니다 AWS. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: Operational Best Practices for Asset Management에서 확인할 수 있습니다.

AWS Backup운영 모범 사례

이 적합성 팩에는 AWS Backup 내부를 기반으로 하는 AWS Config 규칙이 포함되어 있습니다 AWS. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 운영 모범 사례에서 사용할 수 있습니다 AWS Backup.

AWS 자격 증명 및 액세스 관리를 위한 운영 모범 사례

템플릿은 GitHub: AWS 자격 증명 및 액세스 관리를 위한 운영 모범 사례에서 사용할 수 있습니다.

AWS Well-Architected Framework 신뢰성 원칙의 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Amazon Web Services의 Well-Architected Framework 신뢰성 원칙과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 원칙의 설계 원칙과 관련이 있습니다. 하나의 Well-Architected Framework 범주는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-1	서비스 할당량과 제약 조건은 어떻게 관리하나요? 클라우드 기반 워크로드 아키텍처에는 서비스 할당량(서비스 한도라고도 함)이 있습니다. 이러한 할당량은 실수로 필요한 것보다 많은 리소스를 프로비저닝하는 것을 방지하고 API 작업에 대한 요청 비율을 제한하여 서비스가 남용되지 않도록 하기 위해 존재합니다. 또한 리소스에도 제약이 따릅니다. 예를 들면, 광섬유	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선

제어 ID	제어 설명	AWS 구성 규칙	지침
	케이블을 통해 비트를 전송할 수 있는 속도나 물리적 디스크의 스토리지 용량 등이 있습니다.		택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
REL-1	서비스 할당량과 제약 조건은 어떻게 관리하나요? 클라우드 기반 워크로드 아키텍처에는 서비스 할당량(서비스 한도라고도 함)이 있습니다. 이러한 할당량은 실수로 필요한 것보다 많은 리소스를 프로비저닝하는 것을 방지하고 API 작업에 대한 요청 비율을 제한하여 서비스가 남용되지 않도록 하기 위해 존재합니다. 또한 리소스에도 제약이 따릅니다. 예를 들면, 섬유 케이블을 통해 비트를 전송할 수 있는 속도나 물리적 디스크의 스토리지 용량 등이 있습니다.	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-1	서비스 할당량과 제약 조건은 어떻게 관리하나요? 클라우드 기반 워크로드 아키텍처에는 서비스 할당량(서비스 한도라고도 함)이 있습니다. 이러한 할당량은 실수로 필요한 것보다 많은 리소스를 프로비저닝하는 것을 방지하고 API 작업에 대한 요청 비율을 제한하여 서비스가 남용되지 않도록 하기 위해 존재합니다. 또한 리소스에도 제약이 따릅니다. 예를 들면, 광섬유 케이블을 통해 비트를 전송할 수 있는 속도나 물리적 디스크의 스토리지 용량 등이 있습니다.	ecs-task-definition-memory-hard-limit	Amazon Elastic Container Service(ECS) 컨테이너에 사용할 수 있는 최대 메모리를 제한하면 컨테이너에 악의적으로 액세스하는 경우 리소스 사용이 남용되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-2	네트워크 토폴로지는 어떻게 계획하나요? 워크로드는 여러 환경에 존재하는 경우가 많습니다. 여기에는 여러 클라우드 환경(퍼블릭 액세스 가능 및 프라이빗)과 기존 데이터 센터 인프라가 포함됩니다. 계획에는 시스템 내부 및 시스템 간 연결, 퍼블릭 IP 주소 관리, 프라이빗 IP 주소 관리 및 도메인 이름 확인과 같은 네트워크 고려 사항이 포함되어야 합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-2	네트워크 토폴로지는 어떻게 계획하나요? 워크로드는 여러 환경에 존재하는 경우가 많습니다. 여기에는 여러 클라우드 환경(퍼블릭 액세스 가능 및 프라이빗)과 기존 데이터 센터 인프라가 포함됩니다. 계획에는 시스템 내부 및 시스템 간 연결, 퍼블릭 IP 주소 관리, 프라이빗 IP 주소 관리 및 도메인 이름 확인과 같은 네트워크 고려 사항이 포함되어야 합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-2	네트워크 토폴로지는 어떻게 계획하나요? 워크로드는 여러 환경에 존재하는 경우가 많습니다. 여기에는 여러 클라우드 환경(퍼블릭 액세스 가능 및 프라이빗)과 기존 데이터 센터 인프라가 포함됩니다. 계획에는 시스템 내부 및 시스템 간 연결, 퍼블릭 IP 주소 관리, 프라이빗 IP 주소 관리 및 도메인 이름 확인과 같은 네트워크 고려 사항이 포함되어야 합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-5	분산 시스템에서 장애를 완화하거나 견딜 수 있도록 상호 작용을 설계하려면 어떻게 해야 하나요? 분산 시스템은 통신 네트워크를 사용하여 서버 또는 서비스와 같은 구성 요소를 상호 연결합니다. 이러한 네트워크에서 데이터 손실이나 지연 시간이 발생하더라도 워크로드는 안정적으로 작동해야 합니다. 분산 시스템의 구성 요소는 다른 구성 요소나 워크로드에 부정적인 영향을 미치지 않는 방식으로 작동해야 합니다. 이러한 모범 사례는 장애를 예방하고 평균 고장 간격(MTBF)을 개선합니다.	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	api-gw-xray-enabled	AWS X-Ray는 애플리케이션이 제공하는 요청에 대한 데이터를 수집하고, 해당 데이터를 보고, 필터링하고, 인사이트를 얻는 데 사용할 수 있는 도구를 제공하여 문제와 최적화 기회를 식별합니다. X-Ray가 활성화되어 있는지 확인하여 요청 및 응답뿐만 아니라 애플리케이션이 다운스트림 AWS 리소스, 마이크로서비스, 데이터베이스 및 HTTP 웹 APIs에 대해 수행하는 호출에 대한 자세한 정보를 볼 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 강화된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	ecs-container-insights-enabled	모니터링은 Amazon Elastic Container Service(ECS) 및 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. 또한 Container Insights는 컨테이너 재시작 오류 같은 진단 정보를 제공하여 문제를 격리하고 신속하게 해결할 수 있도록 도와줍니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-6	워크로드 리소스는 어떻게 모니터링하나요? 로그와 지표는 워크로드 상태를 파악할 수 있는 강력한 도구입니다. 로그와 지표를 모니터링하고 임계값을 초과하거나 중요한 이벤트가 발생할 경우 알림을 보내도록 워크로드를 구성할 수 있습니다. 모니터링을 통해 워크로드가 저성능 임계값을 초과하거나 장애가 발생하는 시점을 인식하고 이에 대응하여 자동으로 복구할 수 있습니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
REL-7	수요 변화에 적응하도록 워크로드를 설계하려면 어떻게 해야 하나요? 확장 가능한 워크로드는 리소스를 자동으로 추가 또는 제거할 수 있는 탄력성을 제공하여 리소스 공급이 특정 시점의 수요와 거의 일치하도록 합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-7	수요 변화에 적응하도록 워크로드를 설계하려면 어떻게 해야 하나요? 확장 가능한 워크로드는 리소스를 자동으로 추가 또는 제거할 수 있는 탄력성을 제공하여 리소스 공급이 특정 시점의 수요와 거의 일치하도록 합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-7	수요 변화에 적응하도록 워크로드를 설계하려면 어떻게 해야 하나요? 확장 가능한 워크로드는 리소스를 자동으로 추가 또는 제거할 수 있는 탄력성을 제공하여 리소스 공급이 특정 시점의 수요와 거의 일치하도록 합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-8	변경은 어떻게 구현하나요? 새로운 기능을 배포하고 워크로드와 운영 환경에서 알려진 소프트웨어를 실행하고 예측 가능한 방식으로 패치를 적용하거나 교체할 수 있도록 하려면 변경 제어가 필요합니다. 이러한 변경이 제어되지 않으면 변경의 영향을 예측하거나 변경으로 인해 발생하는 문제를 해결하는 것이 어려워집니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-8	변경은 어떻게 구현하나요? 새로운 기능을 배포하고 워크로드와 운영 환경에서 알려진 소프트웨어를 실행하고 예측 가능한 방식으로 패치를 적용하거나 교체할 수 있도록 하려면 변경 제어가 필요합니다. 이러한 변경이 제어되지 않으면 변경의 영향을 예측하거나 변경으로 인해 발생하는 문제를 해결하는 것이 어려워집니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
REL-8	변경은 어떻게 구현하나요? 새로운 기능을 배포하고 워크로드와 운영 환경에서 알려진 소프트웨어를 실행하고 예측 가능한 방식으로 패치를 적용하거나 교체할 수 있도록 하려면 변경 제어가 필요합니다. 이러한 변경이 제어되지 않으면 변경의 영향을 예측하거나 변경으로 인해 발생하는 문제를 해결하는 것이 어려워집니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-8	변경은 어떻게 구현하나요? 새로운 기능을 배포하고 워크로드와 운영 환경에서 알려진 소프트웨어를 실행하고 예측 가능한 방식으로 패치를 적용하거나 교체할 수 있도록 하려면 변경 제어가 필요합니다. 이러한 변경이 제어되지 않으면 변경의 영향을 예측하거나 변경으로 인해 발생하는 문제를 해결하는 것이 어려워집니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장되어 있을 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
REL-9	데이터는 어떻게 백업하나요? 복구 시간 목표(RTO) 및 복구 지점 목표(RPO)에 대한 요구 사항을 충족하도록 데이터, 애플리케이션 및 구성을 백업합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-10	장애 격리를 사용하여 워크로드를 보호하려면 어떻게 해야 하나요? 장애 격리 경계는 워크로드 내에서 발생하는 장애의 영향을 한정된 수의 구성 요소로 제한합니다. 경계 외부의 구성 요소는 장애의 영향을 받지 않습니다. 장애 격리 경계를 여러 개 사용하면 워크로드에 미치는 영향을 제한할 수 있습니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
REL-10	장애 격리를 사용하여 워크로드를 보호하려면 어떻게 해야 하나요? 장애 격리 경계는 워크로드 내에서 발생하는 장애의 영향을 한정된 수의 구성 요소로 제한합니다. 경계 외부의 구성 요소는 장애의 영향을 받지 않습니다. 장애 격리 경계를 여러 개 사용하면 워크로드에 미치는 영향을 제한할 수 있습니다.	clb-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-10	장애 격리를 사용하여 워크로드를 보호하려면 어떻게 해야 하나요? 장애 격리 경계는 워크로드 내에서 발생하는 장애의 영향을 한정된 수의 구성 요소로 제한합니다. 경계 외부의 구성 요소는 장애의 영향을 받지 않습니다. 장애 격리 경계를 여러 개 사용하면 워크로드에 미치는 영향을 제한할 수 있습니다.	elbv2-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.
REL-10	장애 격리를 사용하여 워크로드를 보호하려면 어떻게 해야 하나요? 장애 격리 경계는 워크로드 내에서 발생하는 장애의 영향을 한정된 수의 구성 요소로 제한합니다. 경계 외부의 구성 요소는 장애의 영향을 받지 않습니다. 장애 격리 경계를 여러 개 사용하면 워크로드에 미치는 영향을 제한할 수 있습니다.	lambda-vpc-multi-az-check	AWS Lambda 함수가 계정의 Virtual Private Cloud(VPC)에 연결되도록 구성된 경우, 최소 두 개의 서로 다른 가용 영역에 AWS Lambda 함수를 배포하여 단일 영역에서 서비스 중단이 발생할 경우 이벤트를 처리할 수 있는 함수인지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-10	장애 격리를 사용하여 워크로드를 보호하려면 어떻게 해야 하나요? 장애 격리 경계는 워크로드 내에서 발생하는 장애의 영향을 한정된 수의 구성 요소로 제한합니다. 경계 외부의 구성 요소는 장애의 영향을 받지 않습니다. 장애 격리 경계를 여러 개 사용하면 워크로드에 미치는 영향을 제한할 수 있습니다.	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service(OpenSearch Service)의 고가용성과 내결함성을 위해서는 최소한 3개 이상의 데이터 노드가 필요합니다. 3개 이상의 데이터 노드가 포함된 OpenSearch Service 도메인을 배포하면 노드에 장애가 발생하더라도 클러스터 운영이 보장됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-10	장애 격리를 사용하여 워크로드를 보호하려면 어떻게 해야 하나요? 장애 격리 경계는 워크로드 내에서 발생하는 장애의 영향을 한정된 수의 구성 요소로 제한합니다. 경계 외부의 구성 요소는 장애의 영향을 받지 않습니다. 장애 격리 경계를 여러 개 사용하면 워크로드에 미치는 영향을 제한할 수 있습니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-10	장애 격리를 사용하여 워크로드를 보호하려면 어떻게 해야 하나요? 장애 격리 경계는 워크로드 내에서 발생하는 장애의 영향을 한정된 수의 구성 요소로 제한합니다. 경계 외부의 구성 요소는 장애의 영향을 받지 않습니다. 장애 격리 경계를 여러 개 사용하면 워크로드에 미치는 영향을 제한할 수 있습니다.	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
REL-10	장애 격리를 사용하여 워크로드를 보호하려면 어떻게 해야 하나요? 장애 격리 경계는 워크로드 내에서 발생하는 장애의 영향을 한정된 수의 구성 요소로 제한합니다. 경계 외부의 구성 요소는 장애의 영향을 받지 않습니다. 장애 격리 경계를 여러 개 사용하면 워크로드에 미치는 영향을 제한할 수 있습니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

템플릿

템플릿은 GitHub: AWS Well-Architected 신뢰성 원칙의 운영 모범 사례에서 사용할 수 있습니다.

AWS Well-Architected Framework 보안 원칙의 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Amazon Web Services의 Well-Architected Framework 보안 원칙과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 원칙의 설계 원칙과 관련이 있습니다. 하나의 Well-Architected Framework 범주는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-1	워크로드는 어떻게 안전하게 운영하나요? 워크로드를 안전하게 운영하려면 모든 보안 영역에 중요한 모범 사례를 적용해야 합니다. 운영 우수성에 대해 조직 및 워크로드 수준에서 정의한 요구 사항 및 프로세스를 모든 영역에 적용하세요. AWS 및 업계 권장 사항과 위협 인텔리전스를 최신 상태로 유지하면 위협 모델 및 제어 목표를 발전시키는 데 도움이 됩니다. 보안 프로세스, 테스트 및 검증을 자동화하면 보안 운영을 확장할 수 있습니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
SEC-1	워크로드는 어떻게 안전하게 운영하나요? 워크로드를 안전하게 운영하려면 모든 보안 영역에 중요한 모범 사례를 적용해야 합니다. 운영 우수성에 대해 조직 및 워크로드 수준	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합

제어 ID	제어 설명	AWS 구성 규칙	지침
	에서 정의한 요구 사항 및 프로세스를 모든 영역에 적용하세요. AWS 및 업계 권장 사항과 위협 인텔리전스를 최신 상태로 유지하면 위협 모델 및 제어 목표를 발전시키는 데 도움이 됩니다. 보안 프로세스, 테스트 및 검증을 자동화하면 보안 운영을 확장할 수 있습니다.		니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
SEC-1	워크로드는 어떻게 안전하게 운영하나요? 워크로드를 안전하게 운영하려면 모든 보안 영역에 중요한 모범 사례를 적용해야 합니다. 운영 우수성에 대해 조직 및 워크로드 수준에서 정의한 요구 사항 및 프로세스를 모든 영역에 적용하세요. AWS 및 업계 권장 사항과 위협 인텔리전스를 최신 상태로 유지하면 위협 모델 및 제어 목표를 발전시키는 데 도움이 됩니다. 보안 프로세스, 테스트 및 검증을 자동화하면 보안 운영을 확장할 수 있습니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-1	워크로드는 어떻게 안전하게 운영하나요? 워크로드를 안전하게 운영하려면 모든 보안 영역에 중요한 모범 사례를 적용해야 합니다. 운영 우수성에 대해 조직 및 워크로드 수준에서 정의한 요구 사항 및 프로세스를 모든 영역에 적용하세요. AWS 및 업계 권장 사항과 위협 인텔리전스를 최신 상태로 유지하면 위협 모델 및 제어 목표를 발전시키는 데 도움이 됩니다. 보안 프로세스, 테스트 및 검증을 자동화하면 보안 운영을 확장할 수 있습니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-1	워크로드는 어떻게 안전하게 운영하나요? 워크로드를 안전하게 운영하려면 모든 보안 영역에 중요한 모범 사례를 적용해야 합니다. 운영 우수성에 대해 조직 및 워크로드 수준에서 정의한 요구 사항 및 프로세스를 모든 영역에 적용하세요. AWS 및 업계 권장 사항과 위협 인텔리전스를 최신 상태로 유지하면 위협 모델 및 제어 목표를 발전시키는 데 도움이 됩니다. 보안 프로세스, 테스트 및 검증을 자동화하면 보안 운영을 확장할 수 있습니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-1	워크로드는 어떻게 안전하게 운영하나요? 워크로드를 안전하게 운영하려면 모든 보안 영역에 중요한 모범 사례를 적용해야 합니다. 운영 우수성에 대해 조직 및 워크로드 수준에서 정의한 요구 사항 및 프로세스를 모든 영역에 적용하세요. AWS 및 업계 권장 사항과 위협 인텔리전스를 최신 상태로 유지하면 위협 모델 및 제어 목표를 발전시키는 데 도움이 됩니다. 보안 프로세스, 테스트 및 검증을 자동화하면 보안 운영을 확장할 수 있습니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-1	워크로드는 어떻게 안전하게 운영하나요? 워크로드를 안전하게 운영하려면 모든 보안 영역에 중요한 모범 사례를 적용해야 합니다. 운영 우수성에 대해 조직 및 워크로드 수준에서 정의한 요구 사항 및 프로세스를 모든 영역에 적용하세요. AWS 및 업계 권장 사항과 위협 인텔리전스를 최신 상태로 유지하면 위협 모델 및 제어 목표를 발전시키는 데 도움이 됩니다. 보안 프로세스, 테스트 및 검증을 자동화하면 보안 운영을 확장할 수 있습니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-1	워크로드는 어떻게 안전하게 운영하나요? 워크로드를 안전하게 운영하려면 모든 보안 영역에 중요한 모범 사례를 적용해야 합니다. 운영 우수성에 대해 조직 및 워크로드 수준에서 정의한 요구 사항 및 프로세스를 모든 영역에 적용하세요. AWS 및 업계 권장 사항과 위협 인텔리전스를 최신 상태로 유지하면 위협 모델 및 제어 목표를 발전시키는 데 도움이 됩니다. 보안 프로세스, 테스트 및 검증을 자동화하면 보안 운영을 확장할 수 있습니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-1	워크로드는 어떻게 안전하게 운영하나요? 워크로드를 안전하게 운영하려면 모든 보안 영역에 중요한 모범 사례를 적용해야 합니다. 운영 우수성에 대해 조직 및 워크로드 수준에서 정의한 요구 사항 및 프로세스를 모든 영역에 적용하세요. AWS 및 업계 권장 사항과 위협 인텔리전스를 최신 상태로 유지하면 위협 모델 및 제어 목표를 발전시키는 데 도움이 됩니다. 보안 프로세스, 테스트 및 검증을 자동화하면 보안 운영을 확장할 수 있습니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-1	워크로드는 어떻게 안전하게 운영하나요? 워크로드를 안전하게 운영하려면 모든 보안 영역에 중요한 모범 사례를 적용해야 합니다. 운영 우수성에 대해 조직 및 워크로드 수준에서 정의한 요구 사항 및 프로세스를 모든 영역에 적용하세요. AWS 및 업계 권장 사항과 위협 인텔리전스를 최신 상태로 유지하면 위협 모델 및 제어 목표를 발전시키는 데 도움이 됩니다. 보안 프로세스, 테스트 및 검증을 자동화하면 보안 운영을 확장할 수 있습니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 컨트롤은 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	secretsmanager-secret-periodic-rotation	이 규칙은 AWS Secrets Manager 보안 암호에 주기적 교체가 활성화되어 있도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	secretsmanager-secret-unused	AWS Secrets Manager에 미사용 자격 증명이 있는 경우 최소 권한 원칙을 위반할 수 있으므로 자격 증명을 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하면 값을 unusedForDays(Config 기본값: 90)로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-2	사람 및 시스템의 ID는 어떻게 관리하나요? 보안 AWS 워크로드를 운영할 때 관리해야 하는 두 가지 유형의 자격 증명이 있습니다. 관리하고 액세스 권한을 부여해야 하는 ID 유형을 이해하면 올바른 ID가 적절한 조건에서 올바른 리소스에 액세스할 수 있도록 보장할 수 있습니다. 인적 자격 증명: 관리자, 개발자, 운영자 및 최종 사용자가 AWS 환경 및 애플리케이션에 액세스하려면 자격 증명이 필요합니다. 이들은 조직의 멤버 또는 협업하고 웹 브라우저, 클라이언트 애플리케이션 또는 대화형 명령줄 도구에서 AWS 리소스와 상호 작용하는 외부 사용자입니다. 기계 ID: 서비스 애플리케이션, 운영 도구 및 워크로드는 예를 들어 데이터를 읽기 위해 AWS 서비스에 요청을 하려면 ID가 필요합니다. 이러한 자격 증명에는 Amazon EC2 인스턴	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스 또는 AWS Lambda 함수와 같은 AWS 환경에서 실행되는 시스템이 포함됩니다. 액세스가 필요한 외부 당사자에 대한 시스템 자격 증명을 관리할 수도 있습니다. 또한 AWS 환경에 액세스해야 AWS 하는 외부의 머신도 있을 수 있습니다.		
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 관리자, 최종 사용자 또는 기타 구성 요소별로 워크로드의 각 구성 요소 또는 리소스에 액세스해야 합니다. 각 구성 요소에 대한 액세스 권한 부여 대상을 명확하게 정의하고 적절한 ID 유형과 인증 및 권한 부여 방법을 선택합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 조직 내 모든 ID에 대한 액세스를 제한하는 공통 제어 기능을 설정합니다. 예를 들어 특정 AWS 리전에 대한 액세스를 제한하거나 운영자가 중앙 보안팀에 사용되는 IAM 역할과 같은 공통 리소스를 삭제하지 못하도록 할 수 있습니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	secretsmanager-secret-unused	AWS Secrets Manager에 미사용 자격 증명이 있는 경우 자격 증명을 비활성화 및/또는 제거해야 합니다. 최소 권한 원칙을 위반할 수 있습니다. 이 규칙을 사용하면 값을 unusedForDays(Config 기본값: 90)로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
SEC-3	사람과 시스템에 대한 권한은 어떻게 관리하나요? 퍼블릭 및 크로스 계정 액세스를 강조하는 결과를 지속적으로 모니터링합니다. 퍼블릭 액세스 및 크로스 계정 액세스를 이러한 유형의 액세스가 필요한 리소스로만 제한하세요.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷의 객체에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-4	보안 이벤트는 어떻게 감지하고 조사하나요? 로그와 지표에서 이벤트를 캡처하고 분석하여 가시성을 확보합니다. 보안 이벤트 및 잠재적 위협에 대해 조치를 취해 워크로드를 보호할 수 있습니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	ec2-instance-multiple-eni-check	이 규칙은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 ENI가 여러 개 있는지 확인합니다. ENI가 여러 개 있으면 이중 홈 인스턴스, 즉 서브넷이 여러 개 있는 인스턴스가 발생할 수 있습니다. 이로 인해 네트워크 보안이 복잡해지고 의도하지 않은 네트워크 경로와 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
SEC-5	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	waf-regional-rule-not-empty	AWS WAF에 비어 있지 않은 규칙이 있는지 확인합니다. 조건이 없는 규칙에는 의도하지 않은 동작이 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	waf-regional-rulegroup-not-empty	AWS WAF에 비어 있지 않은 규칙 그룹이 있는지 확인합니다. 규칙 그룹이 비어 있으면 의도하지 않은 동작이 발생할 수 있습니다.
SEC-5	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-5	네트워크 리소스는 어떻게 보호하나요? 인터넷이든 프라이빗 네트워크이든 관계없이 특정 형태의 네트워크 연결이 있는 모든 워크로드에는 외부 및 내부 네트워크 기반 위협으로부터 보호하는 데 도움이 되는 다중 방어 계층이 필요합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository(ECR) 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ecs-container-insights-enabled	모니터링은 Amazon Elastic Container Service(ECS) 및 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. 또한 Container Insights는 컨테이너 재시작 오류 같은 진단 정보를 제공하여 문제를 격리하고 신속하게 해결할 수 있도록 도와줍니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. AWS Fargate 플랫폼 버전에 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ec2-instance-multiple-eni-check	이 규칙은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 ENI가 여러 개 있는지 확인합니다. ENI가 여러 개 있으면 이중 홈 인스턴스, 즉 서브넷이 여러 개 있는 인스턴스가 발생할 수 있습니다. 이로 인해 네트워크 보안이 복잡해지고 의도하지 않은 네트워크 경로와 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ec2-security-group-attached-to-eni-periodic	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
SEC-6	컴퓨팅 리소스는 어떻게 보호하나요? 워크로드의 컴퓨팅 리소스를 외부 및 내부 위협으로부터 보호할 수 있는 다중 방어 계층이 필요합니다. 컴퓨팅 리소스에는 EC2 인스턴스, 컨테이너, AWS Lammbda 함수, 데이터베이스 서비스, IoT 디바이스 등이 포함됩니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 다수의 제어를 구현하여 저장 데이터를 보호하고 무단 액세스 또는 처리 오류의 위험을 줄입니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	codebuild-project-s3-logs-encrypted	저장 시 민감한 데이터를 보호하려면 Amazon S3에 저장된 AWS CodeBuild 로그에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-8	저장 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 처리 오류의 위험을 줄여 저장 데이터를 보호합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SEC-9	전송 중 데이터는 어떻게 보호하나요? 여러 제어를 구현하여 무단 액세스 또는 손실의 위험을 줄여 전송 중인 데이터를 보호합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

템플릿

템플릿은 GitHub: AWS Well-Architected Security Pillar 운영 모범 사례에서 사용할 수 있습니다.

BCP 및 DR 운영 모범 사례

이 적합성 팩에는 BCP 및 DR을 기반으로 하는 AWS Config 규칙이 포함되어 있습니다 AWS. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: Operational Best Practices for BCP and DR에서 확인할 수 있습니다.

BNM RMiT 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Bank Negara Malaysia(BNM) 기술 위험 관리(RMiT)와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 BNM RMiT 제어와 관련이 있습니다. BNM RMiT 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	[api-gw-cache-enabled-and-encrypted](#)	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.18	금융 기관은 정보의 기밀성, 무결성, 인증, 권한 부여, 부인 방지를 보호하기 위해 사용되는 기술과 관련된 암호화 제어를 실사하고 평가해야 합니다. 자체 암호화 키를 생성하지 않는 금융 기관은 암호화 키를 관리할 수 있는 강력한 제어 및 프로세스를 마련하기 위한 적절한 조치를 취해야 합니다. 이를 위해 제3자의 평가에 의존해야 하는 경우, 금융 기관은 그러한 의존이 금융 기관의 위험 수용 범위 및 허용 범위에 부합하는지 여부를 고려해야 합니다. 금융 기관은 암호화 제어를 지원하는 데 필요한 시스템 리소스와 암호화된 데이터의 네트워크 트래픽 가시성이 저하될 위험도 충분히 고려해야 합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.20	금융 기관은 위험 수준에 따라 인증 기관에서 발급한 인증서에 퍼블릭 암호화 키를 저장해야 합니다. 고객과 관련된 이러한 인증서는 공인 인증 기관에서 발급해야 합니다. 금융 기관은 이러한 인증서를 사용한 인증 및 서명 프로토콜의 구현을 강력히 보호함으로써 사용자 인증서에 해당하는 개인 암호화 키의 사용이 법적 구속력을 갖고 반박할 수 없도록 해야 합니다. 이러한 인증서의 최초 발급 및 후속 갱신은 업계 모범 사례 및 관련 법률/규제 사양에 부합해야 합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.20	금융 기관은 위험 수준에 따라 인증 기관에서 발급한 인증서에 퍼블릭 암호화 키를 저장해야 합니다. 고객과 관련된 이러한 인증서는 공인 인증 기관에서 발급해야 합니다. 금융 기관은 이러한 인증서를 사용한 인증 및 서명 프로토콜의 구현을 강력히 보호함으로써 사용자 인증서에 해당하는 개인 암호화 키의 사용이 법적 구속력을 갖고 반박할 수 없도록 해야 합니다. 이러한 인증서의 최초 발급 및 후속 갱신은 업계 모범 사례 및 관련 법률/규제 사양에 부합해야 합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.27	금융 기관은 주요 프로세스 및 서비스의 용량 사용률과 성능을 추적하는 실시간 모니터링 메커니즘을 구축해야 합니다. 이러한 모니터링 메커니즘은 관리자에게 시기적절하고 실행 가능한 알림을 제공할 수 있어야 합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.27	금융 기관은 주요 프로세스 및 서비스의 용량 사용률과 성능을 추적하는 실시간 모니터링 메커니즘을 구축해야 합니다. 이러한 모니터링 메커니즘은 관리자에게 시기적절하고 실행 가능한 알림을 제공할 수 있어야 합니다.	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.27	금융 기관은 주요 프로세스 및 서비스의 용량 사용률과 성능을 추적하는 실시간 모니터링 메커니즘을 구축해야 합니다. 이러한 모니터링 메커니즘은 관리자에게 시기적절하고 실행 가능한 알림을 제공할 수 있어야 합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
10.27	금융 기관은 주요 프로세스 및 서비스의 용량 사용률과 성능을 추적하는 실시간 모니터링 메커니즘을 구축해야 합니다. 이러한 모니터링 메커니즘은 관리자에게 시기적절하고 실행 가능한 알림을 제공할 수 있어야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.27	금융 기관은 주요 프로세스 및 서비스의 용량 사용률과 성능을 추적하는 실시간 모니터링 메커니즘을 구축해야 합니다. 이러한 모니터링 메커니즘은 관리자에게 시기적절하고 실행 가능한 알림을 제공할 수 있어야 합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.27	금융 기관은 주요 프로세스 및 서비스의 용량 사용률과 성능을 추적하는 실시간 모니터링 메커니즘을 구축해야 합니다. 이러한 모니터링 메커니즘은 관리자에게 시기적절하고 실행 가능한 알림을 제공할 수 있어야 합니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
10.27	금융 기관은 주요 프로세스 및 서비스의 용량 사용률과 성능을 추적하는 실시간 모니터링 메커니즘을 구축해야 합니다. 이러한 모니터링 메커니즘은 관리자에게 시기적절하고 실행 가능한 알림을 제공할 수 있어야 합니다.	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.
10.27	금융 기관은 주요 프로세스 및 서비스의 용량 사용률과 성능을 추적하는 실시간 모니터링 메커니즘을 구축해야 합니다. 이러한 모니터링 메커니즘은 관리자에게 시기적절하고 실행 가능한 알림을 제공할 수 있어야 합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.27	금융 기관은 주요 프로세스 및 서비스의 용량 사용률과 성능을 추적하는 실시간 모니터링 메커니즘을 구축해야 합니다. 이러한 모니터링 메커니즘은 관리자에게 시기적절하고 실행 가능한 알림을 제공할 수 있어야 합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.34	금융 기관은 잠재적 네트워크 장애 및 사이버 위협으로부터 중요 시스템을 보호하기 위해 중요 시스템의 네트워크 서비스가 안정적이고 SPOF가 없는지 확인해야 합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
10.34	금융 기관은 잠재적 네트워크 장애 및 사이버 위협으로부터 중요 시스템을 보호하기 위해 중요 시스템의 네트워크 서비스가 안정적이고 SPOF가 없는지 확인해야 합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.35	금융 기관은 실시간 네트워크 대역폭 모니터링 프로세스와 이에 상응하는 네트워크 서비스 복원력 지표를 수립하여 대역폭 과다 사용과 대역폭 혼잡 및 네트워크 장애로 인한 시스템 장애에 플래그를 지정해야 합니다. 여기에는 추세와 이상 현상을 탐지하기 위한 트래픽 분석이 포함됩니다.	api-gw-xray-enabled	AWS X-Ray는 애플리케이션이 제공하는 요청에 대한 데이터를 수집하고, 해당 데이터를 보고, 필터링하고, 인사이트를 얻는 데 사용할 수 있는 도구를 제공하여 문제와 최적화 기회를 식별합니다. X-Ray가 활성화되어 있는지 확인하여 요청 및 응답뿐만 아니라 애플리케이션이 다운스트림 AWS 리소스, 마이크로서비스, 데이터베이스 및 HTTP 웹 APIs에 대해 수행하는 호출에 대한 자세한 정보를 볼 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.35	금융 기관은 실시간 네트워크 대역폭 모니터링 프로세스와 이에 상응하는 네트워크 서비스 복원력 지표를 수립하여 대역폭 과다 사용과 대역폭 혼잡 및 네트워크 장애로 인한 시스템 장애에 플래그를 지정해야 합니다. 여기에는 추세와 이상 현상을 탐지하기 위한 트래픽 분석이 포함됩니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.35	금융 기관은 실시간 네트워크 대역폭 모니터링 프로세스와 이에 상응하는 네트워크 서비스 복원력 지표를 수립하여 대역폭 과다 사용과 대역폭 혼잡 및 네트워크 장애로 인한 시스템 장애에 플래그를 지정해야 합니다. 여기에는 추세와 이상 현상을 탐지하기 위한 트래픽 분석이 포함됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
10.35	금융 기관은 실시간 네트워크 대역폭 모니터링 프로세스와 이에 상응하는 네트워크 서비스 복원력 지표를 수립하여 대역폭 과다 사용과 대역폭 혼잡 및 네트워크 장애로 인한 시스템 장애에 플래그를 지정해야 합니다. 여기에는 추세와 이상 현상을 탐지하기 위한 트래픽 분석이 포함됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.36	금융 기관의 중요 시스템을 지원하는 네트워크 서비스는 데이터의 기밀성, 무결성, 가용성을 보장하도록 설계되고 구현되어야 합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.36	금융 기관의 중요 시스템을 지원하는 네트워크 서비스는 데이터의 기밀성, 무결성, 가용성을 보장하도록 설계되고 구현되어야 합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
10.36	금융 기관의 중요 시스템을 지원하는 네트워크 서비스는 데이터의 기밀성, 무결성, 가용성을 보장하도록 설계되고 구현되어야 합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.36	금융 기관의 중요 시스템을 지원하는 네트워크 서비스는 데이터의 기밀성, 무결성, 가용성을 보장하도록 설계되고 구현되어야 합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
10.36	금융 기관의 중요 시스템을 지원하는 네트워크 서비스는 데이터의 기밀성, 무결성, 가용성을 보장하도록 설계되고 구현되어야 합니다.	nlb-cross-zone-load-balancing-enabled	Network Load Balancer(NLB)의 영역 간 로드 밸런싱 활성화는 적절한 용량 및 가용성 유지에 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.38	금융 기관은 조사 및 포렌식 목적으로 충분하고 관련성이 높은 네트워크 디바이스 로그를 최소 3년 동안 유지해야 합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.51	금융 기관은 클라우드 서비스를 사용할 때 고객 및 거래 상대방 정보와 독점 데이터에 대한 적절한 보호 조치를 구현하여 무단 공개 및 액세스를 방지해야 합니다. 여기에는 관련 암호화 키 관리를 비롯하여 클라우드에 호스팅되는 고객 및 거래 상대방 정보, 독점 데이터, 서비스와 관련된 모든 데이터의 소유권, 제어, 관리를 유지하는 것이 포함됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
10.52	금융 기관은 사용자(내부 사용자와 타사 서비스 제공자 등 외부 사용자)의 식별, 인증, 권한 부여를 위한 적절한 액세스 제어 정책을 구현해야 합니다. 이 액세스 제어 정책은 기술 시스템에 대한 무단 액세스 위험 수준에 상응하는 논리적 액세스 제어와 물리적 기술 액세스 제어를 모두 해결해야 합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.53(b)(h)(i)	금융 기관은 10.52항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (b) '최소 권한' 액세스 권한을 사용하거나 필요한 경우에 한해 합법적인 사용자에게 역할 수행에 충분한 최소한의 권한만 부여하고, (h) 여러 사용자의 사용자 ID 및 암호 공유를 제한 및 제어하고, (i) 보다 개인 식별이 쉬운 ID를 사용하도록 일반 사용자 ID 명명 규칙의 사용을 제어합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
10.53(b)	금융 기관은 10.52항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (b) '최소 권한' 액세스 권한을 사용하거나 필요한 경우에 한해 합법적인 사용자에게 역할 수행에 충분한 최소한의 권한만 부여합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.53(b)	금융 기관은 10.52항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (b) '최소 권한' 액세스 권한을 사용하거나 필요한 경우에 한해 합법적인 사용자에게 역할 수행에 충분한 최소한의 권한만 부여합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.53(b)	금융 기관은 10.52항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (b) '최소 권한' 액세스 권한을 사용하거나 필요한 경우에 한해 합법적인 사용자에게 역할 수행에 충분한 최소한의 권한만 부여합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.53(b)	금융 기관은 10.52항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (b) '최소 권한' 액세스 권한을 사용하거나 필요한 경우에 한해 합법적인 사용자에게 역할 수행에 충분한 최소한의 권한만 부여합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
10.53(b)	금융 기관은 10.52항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (b) '최소 권한' 액세스 권한을 사용하거나 필요한 경우에 한해 합법적인 사용자에게 역할 수행에 충분한 최소한의 권한만 부여합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.53(b)	금융 기관은 10.52항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (b) '최소 권한' 액세스 권한을 사용하거나 필요한 경우에 한해 합법적인 사용자에게 역할 수행에 충분한 최소한의 권한만 부여합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
10.53(b)	금융 기관은 10.52항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (b) '최소 권한' 액세스 권한을 사용하거나 필요한 경우에 한해 합법적인 사용자에게 역할 수행에 충분한 최소한의 권한만 부여합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.53(c)(f)	금융 기관은 10.52항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (c) 서비스 제공자에게 부여된 액세스 권한을 포함하여 특정 기간으로 액세스를 제한하는 시간 제한 액세스 권한을 사용하고, (f) 원격 액세스를 포함한 중요한 활동에 대해서는 더 강력한 인증을 채택합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
10.53(f)(h)	금융 기관은 10.52항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (f) 원격 액세스를 포함한 중요한 활동에 대해서는 더 강력한 인증을 채택하고, (h) 여러 사용자의 사용자 ID 및 암호 공유를 제한 및 제어합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
10.53(f)(h)	금융 기관은 10.54항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (f) 원격 액세스를 포함한 중요한 활동에 대해서는 더 강력한 인증을 채택하고, (h) 여러 사용자의 사용자 ID 및 암호 공유를 제한 및 제어합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.53(f)(h)	금융 기관은 10.54항을 준수할 때 액세스 제어 정책에서 다음 원칙을 고려해야 합니다. (f) 원격 액세스를 포함한 중요한 활동에 대해서는 더 강력한 인증을 채택하고, (h) 여러 사용자의 사용자 ID 및 암호 공유를 제한 및 제어합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.54	금융 기관은 강력한 인증 프로세스를 사용하여 사용 중인 자격 증명의 신뢰성을 보장해야 합니다. 인증 메커니즘은 기능의 중요도에 상응해야 하며, 사용자가 알고 있는 것(예: 암호, PIN), 사용자가 가지고 있는 것(예: 스마트 카드, 보안 디바이스), 사용자 고유의 것(예: 지문 또는 망막 패턴 등 생체 인식 특성) 등 세 가지 기본 인증 요소 중 적어도 하나 이상을 채택해야 합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.54	금융 기관은 강력한 인증 프로세스를 사용하여 사용 중인 자격 증명의 신뢰성을 보장해야 합니다. 인증 메커니즘은 기능의 중요도에 상응해야 하며, 사용자가 알고 있는 것(예: 암호, PIN), 사용자가 가지고 있는 것(예: 스마트 카드, 보안 디바이스), 사용자 고유의 것(예: 지문 또는 망막 패턴 등 생체 인식 특성) 등 세 가지 기본 인증 요소 중 적어도 하나 이상을 채택해야 합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.54	금융 기관은 강력한 인증 프로세스를 사용하여 사용 중인 자격 증명의 신뢰성을 보장해야 합니다. 인증 메커니즘은 기능의 중요도에 상응해야 하며, 사용자가 알고 있는 것(예: 암호, PIN), 사용자가 가지고 있는 것(예: 스마트 카드, 보안 디바이스), 사용자 고유의 것(예: 지문 또는 망막 패턴 등 생체 인식 특성) 등 세 가지 기본 인증 요소 중 적어도 하나 이상을 채택해야 합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.55	금융 기관은 진화하는 공격에 대한 복원력을 강화하기 위해 암호 관행을 정기적으로 검토 및 조정해야 합니다. 여기에는 효과적이고 안전한 암호 생성이 포함됩니다. 생성된 암호가 강력한지 확인할 수 있는 적절한 제어 기능이 있어야 합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
10.56	둘 이상의 요소에 의존하는 인증 방법은 일반적으로 단일 요소 시스템보다 손상시키기가 더 어렵습니다. 이러한 점을 고려할 때 금융 기관은 특히 고위험 시스템이나 'Single Sign-On' 시스템에서 보다 신뢰할 수 있고 강력한 사기 방지 기능을 제공하는 다중 인증(MFA)을 적절하게 설계하고 구현하는 것이 좋습니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
10.56	둘 이상의 요소에 의존하는 인증 방법은 일반적으로 단일 요소 시스템보다 손상시키기가 더 어렵습니다. 이러한 점을 고려할 때 금융 기관은 특히 고위험 시스템이나 'Single Sign-On' 시스템에서 보다 신뢰할 수 있고 강력한 사기 방지 기능을 제공하는 다중 인증(MFA)을 적절하게 설계하고 구현하는 것이 좋습니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.56	둘 이상의 요소에 의존하는 인증 방법은 일반적으로 단일 요소 시스템보다 손상시키기가 더 어렵습니다. 이러한 점을 고려할 때 금융 기관은 특히 고위험 시스템이나 'Single Sign-On' 시스템에서 보다 신뢰할 수 있고 강력한 사기 방지 기능을 제공하는 다중 인증(MFA)을 적절하게 설계하고 구현하는 것이 좋습니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.59	금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 액세스 제어를 효과적으로 관리 및 모니터링하고, (b) 감사 및 조사를 위해 중요 시스템에서의 사용자 활동을 기록해야 합니다. 활동 로그는 최소 3년 동안 유지되어야 하며 시기적절하게 정기적으로 검토해야 합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
10.60	10.59항에 따른 요구사항을 충족하기 위해 대형 금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 사용자 액세스를 효과적으로 관리 및 모니터링할 수 있는 자격 증명 액세스 관리 시스템을 구축하고, (b) 이상 현상을 플래그 지정하기 위한 자동화된 감사 도구를 배포해야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.60	10.61항에 따른 요구 사항을 충족하기 위해 대형 금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 사용자 액세스를 효과적으로 관리 및 모니터링할 수 있는 자격 증명 액세스 관리 시스템을 구축하고, (b) 이상 현상을 플래그 지정하기 위한 자동화된 감사 도구를 배포해야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.60	10.61항에 따른 요구 사항을 충족하기 위해 대형 금융 기관은 (a) 엔터프라이즈 전체 시스템에 대한 사용자 액세스를 효과적으로 관리 및 모니터링할 수 있는 자격 증명 액세스 관리 시스템을 구축하고, (b) 이상 현상을 플래그 지정하기 위한 자동화된 감사 도구를 배포해야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.61	금융 기관은 알려진 보안 취약성이나 수명이 종료된(EOL) 기술 시스템이 있는 오래된 시스템에서 중요 시스템이 실행되지 않도록 해야 합니다. 이와 관련하여 금융 기관은 식별된 기능, 즉 (a) 최신 패치 릴리스를 지속적으로 모니터링하고 적시에 구현하며, (b) 추가 개선 조치를 위해 EOL에 가까워지고 있는 중요 기술 시스템을 식별하는 기능에 책임을 명확히 할당해야 합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.61	금융 기관은 알려진 보안 취약성이나 수명이 종료된(EOL) 기술 시스템이 있는 오래된 시스템에서 중요 시스템이 실행되지 않도록 해야 합니다. 이와 관련하여 금융 기관은 식별된 기능, 즉 (a) 최신 패치 릴리스를 지속적으로 모니터링하고 적시에 구현하며, (b) 추가 개선 조치를 위해 EOL에 가까워지고 있는 중요 기술 시스템을 식별하는 기능에 책임을 명확히 할당해야 합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.61	금융 기관은 알려진 보안 취약성이나 수명이 종료된(EOL) 기술 시스템이 있는 오래된 시스템에서 중요 시스템이 실행되지 않도록 해야 합니다. 이와 관련하여 금융 기관은 식별된 기능, 즉 (a) 최신 패치 릴리스를 지속적으로 모니터링하고 적시에 구현하며, (b) 추가 개선 조치를 위해 EOL에 가까워지고 있는 중요 기술 시스템을 식별하는 기능에 책임을 명확히 할당해야 합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.61	금융 기관은 알려진 보안 취약성이나 수명이 종료된(EOL) 기술 시스템이 있는 오래된 시스템에서 중요 시스템이 실행되지 않도록 해야 합니다. 이와 관련하여 금융 기관은 식별된 기능, 즉 (a) 최신 패치 릴리스를 지속적으로 모니터링하고 적시에 구현하며, (b) 추가 개선 조치를 위해 EOL에 가까워지고 있는 중요 기술 시스템을 식별하는 기능에 책임을 명확히 할당해야 합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.61	금융 기관은 알려진 보안 취약성이나 수명이 종료된(EOL) 기술 시스템이 있는 오래된 시스템에서 중요 시스템이 실행되지 않도록 해야 합니다. 이와 관련하여 금융 기관은 식별된 기능, 즉 (a) 최신 패치 릴리스를 지속적으로 모니터링하고 적시에 구현하며, (b) 추가 개선 조치를 위해 EOL에 가까워지고 있는 중요 기술 시스템을 식별하는 기능에 책임을 명확히 할당해야 합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.64(a)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (a) 고객과 거래 상대방 정보 및 거래의 기밀성과 무결성	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(b)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (b) 서비스 중단을 최소화하면서 채널 및 디바이스가 제공하는 서비스의 신뢰성	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
10.64(b)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (b) 서비스 중단을 최소화하면서 채널 및 디바이스가 제공하는 서비스의 신뢰성	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(b)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (b) 서비스 중단을 최소화하면서 채널 및 디바이스가 제공하는 서비스의 신뢰성	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
10.64(b)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (b) 서비스 중단을 최소화하면서 채널 및 디바이스가 제공하는 서비스의 신뢰성	nlb-cross-zone-load-balancing-enabled	Network Load Balancer(NLB)의 영역 간 로드 밸런싱 활성화는 적절한 용량 및 가용성 유지에 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(b)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (b) 서비스 중단을 최소화하면서 채널 및 디바이스가 제공하는 서비스의 신뢰성	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(b)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (b) 서비스 중단을 최소화하면서 채널 및 디바이스가 제공하는 서비스의 신뢰성	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(b)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (b) 서비스 중단을 최소화하면서 채널 및 디바이스가 제공하는 서비스의 신뢰성	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(b)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (b) 서비스 중단을 최소화하면서 채널 및 디바이스가 제공하는 서비스의 신뢰성	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
10.64(d)	금융 기관은 디지털 서비스를 제공할 때 다음을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (d) 충분한 감사 추적 및 변칙 거래 모니터링	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.64(e)	금융 기관은 디지털 서비스를 제공할 때 다음 사항을 보장하는 강력한 기술 보안 제어를 구현해야 합니다. (e) 인시던트 또는 서비스 중단 전에 복구 지점을 식별하고 되돌릴 수 있는 능력	s3-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Simple Storage Service(S3) 버킷이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.7	금융 기관은 기술 인프라의 이상 활동을 지속적이고 사전 예방적으로 모니터링하고 적시에 탐지할 수 있도록 지원하는 효과적인 도구를 배포해야 합니다. 모니터링 범위는 지원 인프라를 포함한 모든 중요 시스템을 포함해야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.7	금융 기관은 기술 인프라의 이상 활동을 지속적이고 사전 예방적으로 모니터링하고 적시에 탐지할 수 있도록 지원하는 효과적인 도구를 배포해야 합니다. 모니터링 범위는 지원 인프라를 포함한 모든 중요 시스템을 포함해야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.8	금융 기관은 사이버 보안 운영이 보안 통제의 잠재적 침해나 보안 태세 약화를 지속적으로 예방하고 탐지하도록 해야 합니다. 대형 금융 기관의 경우, 여기에는 모든 중요 시스템을 지원하는 외부 및 내부 네트워크 구성 요소에 대한 분기별 취약성 평가 수행이 포함되어야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.8	금융 기관은 사이버 보안 운영이 보안 통제의 잠재적 침해나 보안 태세 약화를 지속적으로 예방하고 탐지하도록 해야 합니다. 대형 금융 기관의 경우, 여기에는 모든 중요 시스템을 지원하는 외부 및 내부 네트워크 구성 요소에 대한 분기별 취약성 평가 수행이 포함되어야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.18(c)(f)	SOC는 다음 기능을 수행할 수 있어야 합니다. (c) 취약성 관리, (f) 위협 인텔리전스 분석 및 운영과 침해 지표 (IOC) 모니터링을 포함한 공격자 및 위협 탐지를 위한 상황 인식 제공. 여기에는 서명이 없고 파일이 없는 맬웨어를 탐지하고 엔드포인트 및 네트워크 계층을 포함하여 보안 위협이 될 수 있는 이상 징후를 식별하기 위한 고급 행동 분석이 포함됩니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.18(c)(f)	SOC는 다음 기능을 수행할 수 있어야 합니다. (c) 취약성 관리, (f) 위협 인텔리전스 분석 및 운영과 침해 지표(IOC) 모니터링을 포함한 공격자 및 위협 탐지를 위한 상황 인식 제공. 여기에는 서명이 없고 파일이 없는 맬웨어를 탐지하고 엔드포인트 및 네트워크 계층을 포함하여 보안 위협이 될 수 있는 이상 징후를 식별하기 위한 고급 행동 분석이 포함됩니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.18(c)(f)	SOC는 다음 기능을 수행할 수 있어야 합니다. (c) 취약성 관리, (f) 위협 인텔리전스 분석 및 운영과 침해 지표 (IOC) 모니터링을 포함한 공격자 및 위협 탐지를 위한 상황 인식 제공. 여기에는 서명이 없고 파일이 없는 맬웨어를 탐지하고 엔드포인트 및 네트워크 계층을 포함하여 보안 위협이 될 수 있는 이상 징후를 식별하기 위한 고급 행동 분석이 포함됩니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 5.1	모든 보안 디바이스의 구성 및 규칙 설정을 정기적으로 검토하세요. 자동화된 도구를 사용하여 구성 및 규칙 설정의 변경 사항을 검토하고 모니터링할 수 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 5.1	모든 보안 디바이스의 구성 및 규칙 설정을 정기적으로 검토하세요. 자동화된 도구를 사용하여 구성 및 규칙 설정의 변경 사항을 검토하고 모니터링할 수 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
부록 5.5(b)	서버 간 외부 네트워크 연결 보안 제어에 다음이 포함되는지 확인합니다. (b) 전송 계층 보안(TLS) 및 가상 프라이빗 네트워크(VPN) IPSec과 같은 보안 터널 사용	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 5.5(b)	서버 간 외부 네트워크 연결 보안 제어에 다음이 포함되는지 확인합니다. (b) 전송 계층 보안(TLS) 및 가상 프라이빗 네트워크(VPN) IPSec과 같은 보안 터널 사용	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
부록 5.5(b)	서버 간 외부 네트워크 연결 보안 제어에 다음이 포함되는지 확인합니다. (b) 전송 계층 보안(TLS) 및 가상 프라이빗 네트워크(VPN) IPSec과 같은 보안 터널 사용	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
부록 5.5(b)	서버 간 외부 네트워크 연결 보안 제어에 다음이 포함되는지 확인합니다. (b) 전송 계층 보안(TLS) 및 가상 프라이빗 네트워크(VPN) IPSec과 같은 보안 터널 사용	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 5.5(b)	서버 간 외부 네트워크 연결 보안 제어에 다음이 포함되는지 확인합니다. (b) 전송 계층 보안(TLS) 및 가상 프라이빗 네트워크(VPN) IPSec과 같은 보안 터널 사용	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
부록 5.5(b)	서버 간 외부 네트워크 연결 보안 제어에 다음이 포함되는지 확인합니다. (b) 전송 계층 보안(TLS) 및 가상 프라이빗 네트워크(VPN) IPSec과 같은 보안 터널 사용	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 5.5(c)	서버 간 외부 네트워크 연결 보안 제어에 다음이 포함되는지 확인합니다. (c) 방화벽, IPS, 바이러스 백신과 같은 적절한 경계 방어 및 보호 기능을 갖춘 스테이징 서버 배포.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
부록 5.5(c)	서버 간 외부 네트워크 연결 보안 제어에 다음이 포함되는지 확인합니다. (c) 방화벽, IPS, 바이러스 백신과 같은 적절한 경계 방어 및 보호 기능을 갖춘 스테이징 서버 배포.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 5.5(c)	서버 간 외부 네트워크 연결 보안 제어에 다음이 포함되는지 확인합니다. (c) 방화벽, IPS, 바이러스 백신과 같은 적절한 경계 방어 및 보호 기능을 갖춘 스테이징 서버 배포.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 5.6	서버 원격 액세스 보안 제어에 다음이 포함되어야 합니다. (a) 보안이 강화되고 잠긴 엔드포인트 디바이스로만 액세스 제한, (b) TLS 및 VPN IPSec과 같은 보안 터널 사용, (c) 방화벽, IPS, 바이러스 백신과 같은 적절한 경계 방어 및 보호 기능을 갖춘 '게이트웨이' 서버 배포, (d) 원격 액세스가 만료되면 즉시 관련 포트 닫기.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
부록 5.6	서버 원격 액세스 보안 제어에 다음이 포함되어야 합니다. (a) 보안이 강화되고 잠긴 엔드포인트 디바이스로만 액세스 제한, (b) TLS 및 VPN IPSec과 같은 보안 터널 사용, (c) 방화벽, IPS, 바이러스 백신과 같은 적절한 경계 방어 및 보호 기능을 갖춘 '게이트웨이' 서버 배포, (d) 원격 액세스가 만료되면 즉시 관련 포트 닫기.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 5.6	서버 원격 액세스 보안 제어에 다음이 포함되어야 합니다. (a) 보안이 강화되고 잠긴 엔드포인트 디바이스로만 액세스 제한, (b) TLS 및 VPN IPSec과 같은 보안 터널 사용, (c) 방화벽, IPS, 바이러스 백신과 같은 적절한 경계 방어 및 보호 기능을 갖춘 '게이트웨이' 서버 배포, (d) 원격 액세스가 만료되면 즉시 관련 포트 닫기.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
부록 5.6	서버 원격 액세스 보안 제어에 다음이 포함되어야 합니다. (a) 보안이 강화되고 잠긴 엔드포인트 디바이스로만 액세스 제한, (b) TLS 및 VPN IPSec과 같은 보안 터널 사용, (c) 방화벽, IPS, 바이러스 백신과 같은 적절한 경계 방어 및 보호 기능을 갖춘 '게이트웨이' 서버 배포, (d) 원격 액세스가 만료되면 즉시 관련 포트 닫기.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 5.6	서버 원격 액세스 보안 제어에 다음이 포함되어야 합니다. (a) 보안이 강화되고 잠긴 엔드포인트 디바이스로만 액세스 제한, (b) TLS 및 VPN IPSec과 같은 보안 터널 사용, (c) 방화벽, IPS, 바이러스 백신과 같은 적절한 경계 방어 및 보호 기능을 갖춘 '게이트웨이' 서버 배포, (d) 원격 액세스가 만료되면 즉시 관련 포트 닫기.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 5.6	서버 원격 액세스 보안 제어에 다음이 포함되어야 합니다. (a) 보안이 강화되고 잠긴 엔드포인트 디바이스로만 액세스 제한, (b) TLS 및 VPN IPSec과 같은 보안 터널 사용, (c) 방화벽, IPS, 바이러스 백신과 같은 적절한 경계 방어 및 보호 기능을 갖춘 '게이트웨이' 서버 배포, (d) 원격 액세스가 만료되면 즉시 관련 포트 닫기.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
부록 10 파트 B - 1 (a)	금융 기관은 강력한 클라우드 아키텍처를 설계하고 해당 설계가 의도한 애플리케이션의 관련 국제 표준을 준수하는지 확인해야 합니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 1 (b)	금융 기관은 제로 트러스트 원칙을 채택하여 '보안 침해 가정' 사고 방식을 채택하고, 마이크로 세분화를 통한 심층 방어, '기본 거부', '최소 권한' 액세스 권한을 적용하고, 해당하는 경우 심층 검사와 지속적 검증을 실시함으로써 사이버 복원력이 뛰어난 아키텍처를 제공하는 것이 좋습니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.
부록 10 파트 B - 1 (b)	금융 기관은 제로 트러스트 원칙을 채택하여 '보안 침해 가정' 사고 방식을 채택하고, 마이크로 세분화를 통한 심층 방어, '기본 거부', '최소 권한' 액세스 권한을 적용하고, 해당하는 경우 심층 검사와 지속적 검증을 실시함으로써 사이버 복원력이 뛰어난 아키텍처를 제공하는 것이 좋습니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 1 (b)	금융 기관은 제로 트러스트 원칙을 채택하여 '보안 침해 가정' 사고 방식을 채택하고, 마이크로 세분화를 통한 심층 방어, '기본 거부', '최소 권한' 액세스 권한을 적용하고, 해당하는 경우 심층 검사와 지속적 검증을 실시함으로써 사이버 복원력이 뛰어난 아키텍처를 제공하는 것이 좋습니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 1 (b)	금융 기관은 제로 트러스트 원칙을 채택하여 '보안 침해 가정' 사고 방식을 채택하고, 마이크로 세분화를 통한 심층 방어, '기본 거부', '최소 권한' 액세스 권한을 적용하고, 해당하는 경우 심층 검사와 지속적 검증을 실시함으로써 사이버 복원력이 뛰어난 아키텍처를 제공하는 것이 좋습니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
부록 10 파트 B - 1 (c)	금융 기관은 클라우드 네트워크 환경의 복잡성을 관리할 때 세분화된 네트워크 보안 및 중앙 집중식 네트워크 제공을 관리하고 모니터링하기 위한 최신 네트워크 아키텍처 접근 방식과 적절한 네트워크 설계 개념 및 솔루션을 사용해야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 1 (c)	금융 기관은 클라우드 네트워크 환경의 복잡성을 관리할 때 세분화된 네트워크 보안 및 중앙 집중식 네트워크 제공을 관리하고 모니터링하기 위한 최신 네트워크 아키텍처 접근 방식과 적절한 네트워크 설계 개념 및 솔루션을 사용해야 합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
부록 10 파트 B - 1 (d)	금융 기관은 물리적 서버, 애플리케이션 또는 데이터를 클라우드 플랫폼으로 마이그레이션하기 위해 안전하고 암호화된 통신 채널을 구축하고 활용해야 합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 1 (d)	금융 기관은 물리적 서버, 애플리케이션 또는 데이터를 클라우드 플랫폼으로 마이그레이션하기 위해 안전하고 암호화된 통신 채널을 구축하고 활용해야 합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 1 (f) i)	외부 애플리케이션 서비스 제공자와의 상호 연결을 위한 금융 기관의 애플리케이션 프로그래밍 인터페이스 (API) 사용이 늘어나면 새로운 서비스 제공의 효율성을 높일 수 있습니다. 그러나 이로 인해 사이버 공격 표면이 확대되고 잘못된 관리로 인해 정보 보안 인시던트의 영향이 증폭될 수 있습니다. 금융 기관은 다음을 비롯한 엄격한 관리 및 제어 메커니즘을 API에 적용해야 합니다. i) API는 단일 장애 지점의 위험을 피할 수 있도록 서비스 복원력을 고려하여 설계되고 적절한 액세스 제어를 통해 안전하게 구성되어야 합니다.	api-gwv2-authorization-type-configured	Amazon API Gateway v2 API 경로에 기본 백엔드 리소스에 대한 무단 액세스를 방지하도록 설정된 권한 부여 유형이 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 1 (f) ii)	외부 애플리케이션 서비스 제공자와의 상호 연결을 위한 금융 기관의 애플리케이션 프로그래밍 인터페이스(API) 사용이 늘어나면 새로운 서비스 제공의 효율성을 높일 수 있습니다. 그러나 이로 인해 사이버 공격 표면이 확대되고 잘못된 관리로 인해 정보 보안 인시던트의 영향이 증폭될 수 있습니다. 금융 기관은 다음을 비롯한 엄격한 관리 및 제어 메커니즘을 API에 적용해야 합니다. ii) 적절한 인시던트 대응 조치를 통해 사이버 공격에 맞서 API를 추적 및 모니터링하고 더 이상 사용하지 않을 때는 적시에 폐기해야 합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 1 (f) ii)	외부 애플리케이션 서비스 제공자와의 상호 연결을 위한 금융 기관의 애플리케이션 프로그래밍 인터페이스 (API) 사용이 늘어나면 새로운 서비스 제공의 효율성을 높일 수 있습니다. 그러나 이로 인해 사이버 공격 표면이 확대되고 잘못된 관리로 인해 정보 보안 인시던트의 영향이 증폭될 수 있습니다. 금융 기관은 다음을 비롯한 엄격한 관리 및 제어 메커니즘을 API에 적용해야 합니다. ii) 적절한 인시던트 대응 조치를 통해 사이버 공격에 맞서 API를 추적 및 모니터링하고 더 이상 사용하지 않을 때는 적시에 폐기해야 합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 2 (b) ii)	금융 기관은 클라우드 서비스의 보안을 개선하기 위해 지속적으로 향상된 클라우드 기능을 활용해야 하며, 특히 금융 기관은 다음이 권장됩니다. ii) 서비스 배포 시 변경 불가능한 인프라 관행을 사용하고 안정적인 최신 소프트웨어 버전으로 새로운 환경을 생성하여 실패 위험을 줄입니다. 클라우드 환경에 대한 지속적인 모니터링에는 변경 불가능한 인프라의 변경 감지 자동화를 통한 규정 준수 검토 개선과 진화하는 사이버 공격 대응이 포함되어야 합니다.	cloudformation-stack-notification-check	기본 AWS 리소스에 대한 의도하지 않은 변경 사항을 감지하려면 Amazon SNS 주제에 이벤트 알림을 보내도록 CloudFormation 스택이 구성되어 있는지 확인합니다.
부록 10 파트 B - 3 (b) vi)	금융 기관은 가상 머신 및 컨테이너 이미지가 적절하게 구성, 강화 및 모니터링되도록 해야 합니다. 여기에는 다음이 포함됩니다. vi) 저장된 이미지는 무단 액세스 및 변경이 있는지 보안 모니터링을 받습니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 5 (a) i)	효과적인 복구 역량의 일환으로 금융 기관은 클라우드 서비스를 포함하도록 기존 백업 및 복구 절차를 확장해야 합니다. 여기에는 다음이 포함됩니다. i) 클라우드 도입 계획 단계에서 백업 및 복구 전략을 정의하고 공식화	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
부록 10 파트 B - 5 (a) i)	효과적인 복구 역량의 일환으로 금융 기관은 클라우드 서비스를 포함하도록 기존 백업 및 복구 절차를 확장해야 합니다. 여기에는 다음이 포함됩니다. i) 클라우드 도입 계획 단계에서 백업 및 복구 전략을 정의하고 공식화	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 5 (a) i)	효과적인 복구 역량의 일환으로 금융 기관은 클라우드 서비스를 포함하도록 기존 백업 및 복구 절차를 확장해야 합니다. 여기에는 다음이 포함됩니다. i) 클라우드 도입 계획 단계에서 백업 및 복구 전략을 정의하고 공식화	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
부록 10 파트 B - 5 (a) i)	효과적인 복구 역량의 일환으로 금융 기관은 클라우드 서비스를 포함하도록 기존 백업 및 복구 절차를 확장해야 합니다. 여기에는 다음이 포함됩니다. i) 클라우드 도입 계획 단계에서 백업 및 복구 전략을 정의하고 공식화	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 5 (a) i)	효과적인 복구 역량의 일환으로 금융 기관은 클라우드 서비스를 포함하도록 기존 백업 및 복구 절차를 확장해야 합니다. 여기에는 다음이 포함됩니다. i) 클라우드 도입 계획 단계에서 백업 및 복구 전략을 정의하고 공식화	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
부록 10 파트 B - 5 (a) i)	효과적인 복구 역량의 일환으로 금융 기관은 클라우드 서비스를 포함하도록 기존 백업 및 복구 절차를 확장해야 합니다. 여기에는 다음이 포함됩니다. i) 클라우드 도입 계획 단계에서 백업 및 복구 전략을 정의하고 공식화	s3-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Simple Storage Service(S3) 버킷이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 5 (b)	금융 기관은 백업 및 복원 절차를 정기적으로 테스트하여 복구 기능을 검증해야 합니다. 백업 절차의 빈도는 시스템의 중요도 및 시스템의 Recovery Point Object(RPO)에 상응해야 합니다. 금융 기관은 백업 실패 시 신속하게 수정 조치를 취해야 합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 5 (c) i)	금융 기관은 다음을 포함하는 백업 구성 설정(해당하는 경우 IaaS 및 PaaS용)을 포함하여 가상 머신 및 컨테이너의 충분한 백업 및 복구를 보장해야 합니다. i) 비즈니스 복구 목표에서 지정한 특정 시점의 가상 머신 및 컨테이너를 복원할 수 있는 기능을 보장	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 5 (d) i)	금융 기관은 클라우드 서비스의 복원력 요구 사항을 평가하고 시스템의 중요도에 상응하는 적절한 조치를 식별하여 극도로 불리한 시나리오에서도 서비스 가용성을 보장해야 합니다. 금융 기관은 서비스 가용성을 보장하고 집중 위험을 완화하기 위해 위험 기반 접근법을 고려하고 적절한 완화 조치를 점진적으로 채택해야 합니다. 실행 가능한 옵션은 다음과 같습니다. i) 클라우드 서비스의 고가용성 및 이중화 기능을 활용하여 운영 데이터 센터가 다양한 가용 영역에서 중복 용량 확보	autoscaling-multiple-az	고가용성을 보장하려면 오토 스케일링이 여러 가용 영역에 걸쳐 있도록 구성되어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 5 (d) i)	금융 기관은 클라우드 서비스의 복원력 요구 사항을 평가하고 시스템의 중요도에 상응하는 적절한 조치를 식별하여 극도로 불리한 시나리오에서도 서비스 가용성을 보장해야 합니다. 금융 기관은 서비스 가용성을 보장하고 집중 위험을 완화하기 위해 위험 기반 접근법을 고려하고 적절한 완화 조치를 점진적으로 채택해야 합니다. 실행 가능한 옵션은 다음과 같습니다. i) 클라우드 서비스의 고가용성 및 이중화 기능을 활용하여 운영 데이터 센터가 다양한 가용 영역에서 중복 용량 확보	elbv2-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 5 (d) i)	금융 기관은 클라우드 서비스의 복원력 요구 사항을 평가하고 시스템의 중요도에 상응하는 적절한 조치를 식별하여 극도로 불리한 시나리오에서도 서비스 가용성을 보장해야 합니다. 금융 기관은 서비스 가용성을 보장하고 집중 위험을 완화하기 위해 위험 기반 접근법을 고려하고 적절한 완화 조치를 점진적으로 채택해야 합니다. 실행 가능한 옵션은 다음과 같습니다. i) 클라우드 서비스의 고가용성 및 이중화 기능을 활용하여 운영 데이터 센터가 다양한 가용 영역에서 중복 용량 확보	lambda-vpc-multi-az-check	AWS Lambda 함수가 계정의 Virtual Private Cloud(VPC)에 연결되도록 구성된 경우, 최소 두 개의 서로 다른 가용 영역에 AWS Lambda 함수를 배포하여 단일 영역에서 서비스 중단이 발생할 경우 이벤트를 처리할 수 있는 함수인지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 5 (d) i)	금융 기관은 클라우드 서비스의 복원력 요구 사항을 평가하고 시스템의 중요도에 상응하는 적절한 조치를 식별하여 극도로 불리한 시나리오에서도 서비스 가용성을 보장해야 합니다. 금융 기관은 서비스 가용성을 보장하고 집중 위험을 완화하기 위해 위험 기반 접근법을 고려하고 적절한 완화 조치를 점진적으로 채택해야 합니다. 실행 가능한 옵션은 다음과 같습니다. i) 클라우드 서비스의 고가용성 및 이중화 기능을 활용하여 운영 데이터 센터가 다양한 가용 영역에서 중복 용량 확보	nlb-cross-zone-load-balancing-enabled	Network Load Balancer(NLB)의 영역 간 로드 밸런싱 활성화는 적절한 용량 및 가용성 유지에 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 5 (d) i)	금융 기관은 클라우드 서비스의 복원력 요구 사항을 평가하고 시스템의 중요도에 상응하는 적절한 조치를 식별하여 극도로 불리한 시나리오에서도 서비스 가용성을 보장해야 합니다. 금융 기관은 서비스 가용성을 보장하고 집중 위험을 완화하기 위해 위험 기반 접근법을 고려하고 적절한 완화 조치를 점진적으로 채택해야 합니다. 실행 가능한 옵션은 다음과 같습니다. i) 클라우드 서비스의 고가용성 및 이중화 기능을 활용하여 운영 데이터센터가 다양한 가용 영역에서 중복 용량 확보	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 5 (d) i)	금융 기관은 클라우드 서비스의 복원력 요구 사항을 평가하고 시스템의 중요도에 상응하는 적절한 조치를 식별하여 극도로 불리한 시나리오에서도 서비스 가용성을 보장해야 합니다. 금융 기관은 서비스 가용성을 보장하고 집중 위험을 완화하기 위해 위험 기반 접근법을 고려하고 적절한 완화 조치를 점진적으로 채택해야 합니다. 실행 가능한 옵션은 다음과 같습니다. i) 클라우드 서비스의 고가용성 및 이중화 기능을 활용하여 운영 데이터 센터가 다양한 가용 영역에서 중복 용량 확보	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터가 캡처될 수 있으므로 저장 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	eks-secrets-encrypted	저장 데이터를 보호하려면 Kubernetes 보안 암호를 암호화하도록 Amazon Elastic Kubernetes Service(EKS) 클러스터가 구성되어야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 8 (a)	금융 기관은 클라우드에 저장된 민감한 데이터의 기밀성과 무결성을 보호하기 위해 적절하고 관련성 있는 암호화 기술을 구현해야 합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
부록 10 파트 B - 8 (d)	클라우드 채택이 증가함에 따라 데이터 보호에 사용되는 많은 암호화 키를 관리하는 것이 더욱 복잡해졌으며 금융 기관에 새로운 과제가 생길 수 있습니다. 금융 기관은 안전하고 확장 가능한 방식으로 키 생성, 저장, 배포를 처리할 수 있는 중앙 집중식 키 관리 시스템의 사용을 포함하여 포괄적이고 중앙 집중화된 키 관리 접근 방식을 채택해야 합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 8 (d)	클라우드 채택이 증가함에 따라 데이터 보호에 사용되는 많은 암호화 키를 관리하는 것이 더욱 복잡해졌으며 금융 기관에 새로운 과제가 생길 수 있습니다. 금융 기관은 안전하고 확장 가능한 방식으로 키 생성, 저장, 배포를 처리할 수 있는 중앙 집중식 키 관리 시스템의 사용을 포함하여 포괄적이고 중앙 집중화된 키 관리 접근 방식을 채택해야 합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 9 (a) ii)	관리 영역은 원격 액세스가 기본적으로 지원되는 클라우드 컴퓨팅과 기존 인프라의 주요 보안 차이점입니다. 이 액세스 계층은 사이버 공격에 취약하여 전체 클라우드 배포의 무결성을 손상시킬 수 있습니다. 이를 고려하여 금융 기관은 관리 영역 액세스에 대한 강력한 제어를 보장해야 합니다. 여기에는 다음이 포함될 수 있습니다. ii) '최소 권한'과 강력한 다중 인증(MFA) 구현(예: 강력한 암호, 소프트 토큰, 권한 있는 액세스 관리 도구 및 메이커 체커 기능)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
부록 10 파트 B - 9 (a) ii)	관리 영역은 원격 액세스가 기본적으로 지원되는 클라우드 컴퓨팅과 기존 인프라의 주요 보안 차이점입니다. 이 액세스 계층은 사이버 공격에 취약하여 전체 클라우드 배포의 무결성을 손상시킬 수 있습니다. 이를 고려하여 금융 기관은 관리 영역 액세스에 대한 강력한 제어를 보장해야 합니다. 여기에는 다음이 포함될 수 있습니다. ii) '최소 권한'과 강력한 다중 인증(MFA) 구현 (예: 강력한 암호, 소프트 토큰, 권한 있는 액세스 관리 도구 및 메이커 체커 기능)	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 9 (a) ii)	관리 영역은 원격 액세스가 기본적으로 지원되는 클라우드 컴퓨팅과 기존 인프라의 주요 보안 차이점입니다. 이 액세스 계층은 사이버 공격에 취약하여 전체 클라우드 배포의 무결성을 손상시킬 수 있습니다. 이를 고려하여 금융 기관은 관리 영역 액세스에 대한 강력한 제어를 보장해야 합니다. 여기에는 다음이 포함될 수 있습니다. ii) '최소 권한'과 강력한 다중 인증(MFA) 구현 (예: 강력한 암호, 소프트 토큰, 권한 있는 액세스 관리 도구 및 메이커 체커 기능)	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 9 (a) ii)	관리 영역은 원격 액세스가 기본적으로 지원되는 클라우드 컴퓨팅과 기존 인프라의 주요 보안 차이점입니다. 이 액세스 계층은 사이버 공격에 취약하여 전체 클라우드 배포의 무결성을 손상시킬 수 있습니다. 이를 고려하여 금융 기관은 관리 영역 액세스에 대한 강력한 제어를 보장해야 합니다. 여기에는 다음이 포함될 수 있습니다. ii) '최소 권한'과 강력한 다중 인증(MFA) 구현 (예: 강력한 암호, 소프트 토큰, 권한 있는 액세스 관리 도구 및 메이커 체커 기능)	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 9 (a) iii)	관리 영역은 원격 액세스가 기본적으로 지원되는 클라우드 컴퓨팅과 기존 인프라의 주요 보안 차이점입니다. 이 액세스 계층은 사이버 공격에 취약하여 전체 클라우드 배포의 무결성을 손상시킬 수 있습니다. 이를 고려하여 금융 기관은 관리 영역 액세스에 대한 강력한 제어 기능을 사용해야 합니다. 여기에는 다음이 포함될 수 있습니다. iii) 권한이 있는 사용자에게 세분화된 권한 할당 사용	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 9 (a) iii)	관리 영역은 원격 액세스가 기본적으로 지원되는 클라우드 컴퓨팅과 기존 인프라의 주요 보안 차이점입니다. 이 액세스 계층은 사이버 공격에 취약하여 전체 클라우드 배포의 무결성을 손상시킬 수 있습니다. 이를 고려하여 금융 기관은 관리 영역 액세스에 대한 강력한 제어 기능을 사용해야 합니다. 여기에는 다음이 포함될 수 있습니다. iii) 권한이 있는 사용자에게 세분화된 권한 할당 사용	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 9 (a) iv)	관리 영역은 원격 액세스가 기본적으로 지원되는 클라우드 컴퓨팅과 기존 인프라의 주요 보안 차이점입니다. 이 액세스 계층은 사이버 공격에 취약하여 전체 클라우드 배포의 무결성을 손상시킬 수 있습니다. 이를 고려하여 금융 기관은 관리 영역 액세스에 대한 강력한 제어 기능을 사용해야 합니다. 여기에는 다음이 포함될 수 있습니다. iv) 권한이 있는 사용자가 수행하는 활동을 지속적으로 모니터링	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 9 (a) iv)	관리 영역은 원격 액세스가 기본적으로 지원되는 클라우드 컴퓨팅과 기존 인프라의 주요 보안 차이점입니다. 이 액세스 계층은 사이버 공격에 취약하여 전체 클라우드 배포의 무결성을 손상시킬 수 있습니다. 이를 고려하여 금융 기관은 관리 영역 액세스에 대한 강력한 제어 기능을 사용해야 합니다. 여기에는 다음이 포함될 수 있습니다. iv) 권한이 있는 사용자가 수행하는 활동을 지속적으로 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
부록 10 파트 B - 12 (a)	금융 기관은 이 정책 문서의 데이터 손실 방지 섹션(11.14~11.16 항)에서 요구하는 대로 클라우드 서비스에 호스팅되는 데이터를 보호해야 합니다. 여기에는 직원이 자신의 디바이스를 사용하여 민감한 데이터에 액세스하도록 허용하는 경우 엔드포인트 풋프린트 확장이 포함됩니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 12 (a)	금융 기관은 이 정책 문서의 데이터 손실 방지 섹션(11.14~11.16 항)에서 요구하는 대로 클라우드 서비스에 호스팅되는 데이터를 보호해야 합니다. 여기에는 직원이 자신의 디바이스를 사용하여 민감한 데이터에 액세스하도록 허용하는 경우 엔드포인트 풋프린트 확장이 포함됩니다.	macie-status-check	Amazon Macie는 기계 학습(ML)과 패턴 일치를 사용하여 Amazon Simple Storage Service(S3) 버킷에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 데이터 보안 서비스입니다.
부록 10 파트 B - 14 (c) i)	금융 기관은 CIRP 개발 과정에서 다음과 같은 추가 조치를 고려해야 합니다. i) 보안 침해 인시던트 탐지 능력을 강화하여 다크 웹에서의 데이터 유출 탐지 기능을 포함하여 효과적인 인시던트 관리 달성	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부록 10 파트 B - 14 (c) i)	금융 기관은 CIRP 개발 과정에서 다음과 같은 추가 조치를 고려해야 합니다. i) 보안 침해 인시던트 탐지 능력을 강화하여 다크 웹에서의 데이터 유출 탐지 기능을 포함하여 효과적인 인시던트 관리 달성	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

템플릿

템플릿은 GitHub: Operational Best Practices for BNM RMiT에서 확인할 수 있습니다.

캐나다 사이버 보안 센터(CCCS) 중간 클라우드 제어 프로필 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 캐나다 사이버 보안 센터(CCCS) 중형 클라우드 제어 프로파일과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 CCCS

Medium Cloud Control Profile 제어와 관련이 있습니다. CCCS Medium Cloud Control Profile 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경

제어 ID	제어 설명	AWS 구성 규칙	지침
			을 제한할 수 있습니다.
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(1)	AC-2 (1) 계정 관리 | 자동 시스템 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(3)	AC-2(3) 계정 관리 | 비활성 계정 비활성화	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-AC-2(3)	AC-2(3) 계정 관리 | 비활성 계정 비활성화	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
CCCS-fPBMM-AC-2(4)	AC-2(4) 계정 관리 | 자동화된 감사 작업	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(4)	AC-2(4) 계정 관리 | 자동화된 감사 작업	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
CCCS-fPBMM-AC-2(4)	AC-2(4) 계정 관리 | 자동화된 감사 작업	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(4)	AC-2(4) 계정 관리 | 자동화된 감사 작업	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(4)	AC-2(4) 계정 관리 | 자동화된 감사 작업	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(4)	AC-2(4) 계정 관리 | 자동화된 감사 작업	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2(4)	AC-2(4) 계정 관리 | 자동화된 감사 작업	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.A	AC-2.A 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.B	AC-2.B 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.C	AC-2.C 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.D	AC-2.D 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.E	AC-2.E 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.F	AC-2.F 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.G	AC-2.G 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.H	AC-2.H 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.I	AC-2.I 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.J	AC-2.J 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-2.K	AC-2.K 계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-3.A	AC-3.A 액세스 적용	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-AC-4(21)	AC-4(21) 정보 흐름 적용 | 정보 흐름의 물리적/논리적 분리	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4(21)	AC-4(21) 정보 흐름 적용 | 정보 흐름의 물리적/논리적 분리	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
CCCS-fPBMM-AC-4(21)	AC-4(21) 정보 흐름 적용 | 정보 흐름의 물리적/논리적 분리	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4(21)	AC-4(21) 정보 흐름 적용 | 정보 흐름의 물리적/논리적 분리	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4(21)	AC-4(21) 정보 흐름 적용 | 정보 흐름의 물리적/논리적 분리	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4(21)	AC-4(21) 정보 흐름 적용 | 정보 흐름의 물리적/논리적 분리	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-AC-4(21)	AC-4(21) 정보 흐름 적용 | 정보 흐름의 물리적/논리적 분리	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-AC-4(21)	AC-4(21) 정보 흐름 적용 | 정보 흐름의 물리적/논리적 분리	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4(21)	AC-4(21) 정보 흐름 적용 | 정보 흐름의 물리적/논리적 분리	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-4.A	AC-4.A 정보 흐름 적용	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CCCS-fPBMM-AC-5.A	AC-5.A 업무 분리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-5.A	AC-5.A 업무 분리	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-5.A	AC-5.A 업무 분리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-5.A	AC-5.A 업무 분리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-5.A	AC-5.A 업무 분리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-6(1)	AC-6(1) 최소 권한 | 보안 기능에 대한 액세스 권한 부여	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(1)	AC-6(1) 최소 권한 | 보안 기능에 대한 액세스 권한 부여	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-6(1)	AC-6(1) 최소 권한 | 보안 기능에 대한 액세스 권한 부여	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(1)	AC-6(1) 최소 권한 | 보안 기능에 대한 액세스 권한 부여	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(1)	AC-6(1) 최소 권한 | 보안 기능에 대한 액세스 권한 부여	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CCCS-fPBMM-AC-6(2)	AC-6(2) 최소 권한 | 비보안 기능에 대한 비권한 액세스	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(2)	AC-6(2) 최소 권한 | 비보안 기능에 대한 비권한 액세스	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
CCCS-fPBMM-AC-6(2)	AC-6(2) 최소 권한 | 비보안 기능에 대한 비권한 액세스	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(2)	AC-6(2) 최소 권한 | 비보안 기능에 대한 비권한 액세스	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(2)	AC-6(2) 최소 권한 | 비보안 기능에 대한 비권한 액세스	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CCCS-fPBMM-AC-6(5)	AC-6(5) 최소 권한 | 권한이 있는 계정	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(5)	AC-6(5) 최소 권한 | 권한이 있는 계정	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
CCCS-fPBMM-AC-6(5)	AC-6(5) 최소 권한 | 권한이 있는 계정	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(5)	AC-6(5) 최소 권한 | 권한이 있는 계정	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CCCS-fPBMM-AC-6(9)	AC-6 (9) 최소 권한 | 권한이 있는 기능의 사용 감사	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(9)	AC-6 (9) 최소 권한 | 권한이 있는 기능의 사용 감사	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
CCCS-fPBMM-AC-6(9)	AC-6 (9) 최소 권한 | 권한이 있는 기능의 사용 감사	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(9)	AC-6 (9) 최소 권한 | 권한이 있는 기능의 사용 감사	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(9)	AC-6 (9) 최소 권한 | 권한이 있는 기능의 사용 감사	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(9)	AC-6 (9) 최소 권한 | 권한이 있는 기능의 사용 감사	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(9)	AC-6 (9) 최소 권한 | 권한이 있는 기능의 사용 감사	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(10)	AC-6(10) 최소 권한 | 권한이 없는 사용자의 권한이 있는 기능 실행 금지	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-AC-6(10)	AC-6(10) 최소 권한 | 권한이 없는 사용자의 권한이 있는 기능 실행 금지	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(10)	AC-6(10) 최소 권한 | 권한이 없는 사용자의 권한이 있는 기능 실행 금지	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
CCCS-fPBMM-AC-6(10)	AC-6(10) 최소 권한 | 권한이 없는 사용자의 권한이 있는 기능 실행 금지	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6(10)	AC-6(10) 최소 권한 | 권한이 없는 사용자의 권한이 있는 기능 실행 금지	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-6.A	AC-6.A 최소 권한	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(1)	AC-17 (1) 원격 액세스 | 자동 모니터링/제어	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
CCCS-fPBMM-AC-17(2)	AC-17(2) 원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(2)	AC-17(2) 원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
CCCS-fPBMM-AC-17(2)	AC-17(2) 원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(2)	AC-17(2) 원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(2)	AC-17(2) 원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-AC-17(2)	AC-17(2) 원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(3)	AC-17(3) 원격 액세스 | 관리형 액세스 제어 지점	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-AC-17(4)	AC-17(4) 원격 액세스 | 권한이 있는 명령/액세스	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(4)	AC-17(4) 원격 액세스 | 권한이 있는 명령/액세스	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17(4)	AC-17(4) 원격 액세스 | 권한이 있는 명령/액세스	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.A	AC-17.A 원격 액세스	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.AA	AC-17.AA 원격 액세스	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AC-17.B	AC-17.B 원격 액세스	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CCCS-fPBMM-AU-2.A	AU-2.A 이벤트 감사	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.A	AU-2.A 이벤트 감사	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
CCCS-fPBMM-AU-2.A	AU-2.A 이벤트 감사	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.A	AU-2.A 이벤트 감사	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AU-2.A	AU-2.A 이벤트 감사	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.A	AU-2.A 이벤트 감사	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.A	AU-2.A 이벤트 감사	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.A	AU-2.A 이벤트 감사	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.A	AU-2.A 이벤트 감사	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-AU-2.A	AU-2.A 이벤트 감사	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.A	AU-2.A 이벤트 감사	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
CCCS-fPBMM-AU-2.B	AU-2.B 이벤트 감사	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.B	AU-2.B 이벤트 감사	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
CCCS-fPBMM-AU-2.B	AU-2.B 이벤트 감사	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.B	AU-2.B 이벤트 감사	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AU-2.B	AU-2.B 이벤트 감사	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.B	AU-2.B 이벤트 감사	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.B	AU-2.B 이벤트 감사	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.B	AU-2.B 이벤트 감사	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.B	AU-2.B 이벤트 감사	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-AU-2.B	AU-2.B 이벤트 감사	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.B	AU-2.B 이벤트 감사	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
CCCS-fPBMM-AU-2.C	AU-2.C 이벤트 감사	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.C	AU-2.C 이벤트 감사	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
CCCS-fPBMM-AU-2.C	AU-2.C 이벤트 감사	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.C	AU-2.C 이벤트 감사	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AU-2.C	AU-2.C 이벤트 감사	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.C	AU-2.C 이벤트 감사	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.C	AU-2.C 이벤트 감사	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.C	AU-2.C 이벤트 감사	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.C	AU-2.C 이벤트 감사	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-AU-2.C	AU-2.C 이벤트 감사	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.C	AU-2.C 이벤트 감사	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
CCCS-fPBMM-AU-2.D	AU-2.D 이벤트 감사	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.D	AU-2.D 이벤트 감사	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
CCCS-fPBMM-AU-2.D	AU-2.D 이벤트 감사	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.D	AU-2.D 이벤트 감사	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AU-2.D	AU-2.D 이벤트 감사	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.D	AU-2.D 이벤트 감사	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.D	AU-2.D 이벤트 감사	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.D	AU-2.D 이벤트 감사	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.D	AU-2.D 이벤트 감사	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-AU-2.D	AU-2.D 이벤트 감사	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-2.D	AU-2.D 이벤트 감사	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
CCCS-fPBMM-AU-3(1)	AU-3(1) 감사 레코드 콘텐츠 | 추가 감사 정보	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3(1)	AU-3(1) 감사 레코드 콘텐츠 | 추가 감사 정보	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
CCCS-fPBMM-AU-3(1)	AU-3(1) 감사 레코드 콘텐츠 | 추가 감사 정보	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3(1)	AU-3(1) 감사 레코드 콘텐츠 | 추가 감사 정보	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AU-3(1)	AU-3(1) 감사 레코드 콘텐츠 | 추가 감사 정보	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3(1)	AU-3(1) 감사 레코드 콘텐츠 | 추가 감사 정보	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3(1)	AU-3(1) 감사 레코드 콘텐츠 | 추가 감사 정보	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3(1)	AU-3(1) 감사 레코드 콘텐츠 | 추가 감사 정보	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-3.A	AU-3.A 감사 레코드 콘텐츠	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-5.A	AU-5.A 감사 처리 실패에 대한 대응	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-5.B	AU-5.B 감사 처리 실패에 대한 대응	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(1)	AU-6(1) 감사 검토, 분석, 보고 | 프로세스 통합	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
CCCS-fPBMM-AU-6(1)	AU-6(1) 감사 검토, 분석, 보고 | 프로세스 통합	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(1)	AU-6(1) 감사 검토, 분석, 보고 | 프로세스 통합	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AU-6(1)	AU-6(1) 감사 검토, 분석, 보고 | 프로세스 통합	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(1)	AU-6(1) 감사 검토, 분석, 보고 | 프로세스 통합	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(1)	AU-6(1) 감사 검토, 분석, 보고 | 프로세스 통합	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-6(3)	AU-6(3) 감사 검토, 분석, 보고 | 감사 리포지토리 상관 관계 분석	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
CCCS-fPBMM-AU-7(1)	AU-7(1) 감사 감소 및 보고서 생성 | 자동 처리	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-8.B	AU-8.B 타임스탬프	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-9(2)	AU-9(2) 감사 정보 보호 | 별도의 물리적 시스템/구성 요소에 감사 백업	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-9(2)	AU-9(2) 감사 정보 보호 | 별도의 물리적 시스템/구성 요소에 감사 백업	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CCCS-fPBMM-AU-9(2)	AU-9(2) 감사 정보 보호 | 별도의 물리적 시스템/구성 요소에 감사 백업	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-9.A	AU-9.A 감사 정보 보호	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
CCCS-fPBMM-AU-9.A	AU-9.A 감사 정보 보호	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-9.A	AU-9.A 감사 정보 보호	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-AU-11.A	AU-11.A 감사 레코드 보존	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
CCCS-fPBMM-AU-11.B	AU-11.B 감사 레코드 보존	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-11.C	AU-11.C 감사 레코드 보존	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.A	AU-12.A 감사 생성	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
CCCS-fPBMM-AU-12.C	AU-12.C 감사 생성	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.C	AU-12.C 감사 생성	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
CCCS-fPBMM-AU-12.C	AU-12.C 감사 생성	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.C	AU-12.C 감사 생성	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-AU-12.C	AU-12.C 감사 생성	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.C	AU-12.C 감사 생성	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.C	AU-12.C 감사 생성	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.C	AU-12.C 감사 생성	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.C	AU-12.C 감사 생성	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-AU-12.C	AU-12.C 감사 생성	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-AU-12.C	AU-12.C 감사 생성	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-3(5)	CA-3(5) 시스템 상호 연결 | 외부 네트워크 연결에 대한 제한	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	api-gw-xray-enabled	AWS X-Ray는 애플리케이션이 제공하는 요청에 대한 데이터를 수집하고, 해당 데이터를 보고, 필터링하고, 인사이트를 얻는 데 사용할 수 있는 도구를 제공하여 문제와 최적화 기회를 식별합니다. X-Ray가 활성화되어 있는지 확인하여 요청 및 응답뿐만 아니라 애플리케이션이 다운스트림 AWS 리소스, 마이크로서비스, 데이터베이스 및 HTTP 웹 APIs에 대해 수행하는 호출에 대한 자세한 정보를 볼 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
CCCS-fPBMM-CA-7.A	CA-7.A 지속적인 모니터링	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	api-gw-xray-enabled	AWS X-Ray는 애플리케이션이 제공하는 요청에 대한 데이터를 수집하고, 해당 데이터를 보고, 필터링하고, 인사이트를 얻는 데 사용할 수 있는 도구를 제공하여 문제와 최적화 기회를 식별합니다. X-Ray가 활성화되어 있는지 확인하여 요청 및 응답뿐만 아니라 애플리케이션이 다운스트림 AWS 리소스, 마이크로서비스, 데이터베이스 및 HTTP 웹 APIs에 대해 수행하는 호출에 대한 자세한 정보를 볼 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
CCCS-fPBMM-CA-7.B	CA-7.B 지속적인 모니터링	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	api-gw-xray-enabled	AWS X-Ray는 애플리케이션이 제공하는 요청에 대한 데이터를 수집하고, 해당 데이터를 보고, 필터링하고, 인사이트를 얻는 데 사용할 수 있는 도구를 제공하여 문제와 최적화 기회를 식별합니다. X-Ray가 활성화되어 있는지 확인하여 요청 및 응답뿐만 아니라 애플리케이션이 다운스트림 AWS 리소스, 마이크로서비스, 데이터베이스 및 HTTP 웹 APIs에 대해 수행하는 호출에 대한 자세한 정보를 볼 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
CCCS-fPBMM-CA-7.C	CA-7.C 지속적인 모니터링	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	api-gw-xray-enabled	AWS X-Ray는 애플리케이션이 제공하는 요청에 대한 데이터를 수집하고, 해당 데이터를 보고, 필터링하고, 인사이트를 얻는 데 사용할 수 있는 도구를 제공하여 문제와 최적화 기회를 식별합니다. X-Ray가 활성화되어 있는지 확인하여 요청 및 응답뿐만 아니라 애플리케이션이 다운스트림 AWS 리소스, 마이크로서비스, 데이터베이스 및 HTTP 웹 APIs에 대해 수행하는 호출에 대한 자세한 정보를 볼 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
CCCS-fPBMM-CA-7.D	CA-7.D 지속적인 모니터링	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	api-gw-xray-enabled	AWS X-Ray는 애플리케이션이 제공하는 요청에 대한 데이터를 수집하고, 해당 데이터를 보고, 필터링하고, 인사이트를 얻는 데 사용할 수 있는 도구를 제공하여 문제와 최적화 기회를 식별합니다. X-Ray가 활성화되어 있는지 확인하여 요청 및 응답뿐만 아니라 애플리케이션이 다운스트림 AWS 리소스, 마이크로서비스, 데이터베이스 및 HTTP 웹 APIs에 대해 수행하는 호출에 대한 자세한 정보를 볼 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
CCCS-fPBMM-CA-7.E	CA-7.E 지속적인 모니터링	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	api-gw-xray-enabled	AWS X-Ray는 애플리케이션이 제공하는 요청에 대한 데이터를 수집하고, 해당 데이터를 보고, 필터링하고, 인사이트를 얻는 데 사용할 수 있는 도구를 제공하여 문제와 최적화 기회를 식별합니다. X-Ray가 활성화되어 있는지 확인하여 요청 및 응답뿐만 아니라 애플리케이션이 다운스트림 AWS 리소스, 마이크로서비스, 데이터베이스 및 HTTP 웹 APIs에 대해 수행하는 호출에 대한 자세한 정보를 볼 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
CCCS-fPBMM-CA-7.F	CA-7.F 지속적인 모니터링	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	api-gw-xray-enabled	AWS X-Ray는 애플리케이션이 제공하는 요청에 대한 데이터를 수집하고, 해당 데이터를 보고, 필터링하고, 인사이트를 얻는 데 사용할 수 있는 도구를 제공하여 문제와 최적화 기회를 식별합니다. X-Ray가 활성화되어 있는지 확인하여 요청 및 응답뿐만 아니라 애플리케이션이 다운스트림 AWS 리소스, 마이크로서비스, 데이터베이스 및 HTTP 웹 APIs에 대해 수행하는 호출에 대한 자세한 정보를 볼 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
CCCS-fPBMM-CA-7.G	CA-7.G 지속적인 모니터링	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CA-9.A	CA-9.A 내부 시스템 연결	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-2.A	CM-2.A 기본 구성	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-2.A	CM-2.A 기본 구성	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-CM-2.A	CM-2.A 기본 구성	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-2.A	CM-2.A 기본 구성	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
CCCS-fPBMM-CM-2.A	CM-2.A 기본 구성	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-2.A	CM-2.A 기본 구성	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-2.A	CM-2.A 기본 구성	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.A	CM-3.A 구성 변경 제어	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.A	CM-3.A 구성 변경 제어	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.B	CM-3.B 구성 변경 제어	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.B	CM-3.B 구성 변경 제어	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.C	CM-3.C 구성 변경 제어	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.C	CM-3.C 구성 변경 제어	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.D	CM-3.D 구성 변경 제어	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.D	CM-3.D 구성 변경 제어	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.E	CM-3.E 구성 변경 제어	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.E	CM-3.E 구성 변경 제어	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.F	CM-3F 구성 변경 제어	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.F	CM-3F 구성 변경 제어	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.G	CM-3.G 구성 변경 제어	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-3.G	CM-3.G 구성 변경 제어	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(1)	CM-5(1) 변경을 위한 액세스 제한 | 자동 액세스 적용/감사	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
CCCS-fPBMM-CM-5(5)	CM-5(5) 변경을 위한 액세스 제한 | 프로덕션/운영 권한 제한	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
CCCS-fPBMM-CM-5.A	CM-5.A 변경을 위한 액세스 제한	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6(1)	CM-6(1) 구성 설정 | 자동화된 중앙 관리/애플리케이션/검증	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6(1)	CM-6(1) 구성 설정 | 자동화된 중앙 관리/애플리케이션/검증	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-CM-6(1)	CM-6(1) 구성 설정 | 자동화된 중앙 관리/애플리케이션/검증	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
CCCS-fPBMM-CM-6.A	CM-6.A 구성 설정	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
CCCS-fPBMM-CM-6.B	CM-6.B 구성 설정	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
CCCS-fPBMM-CM-6.C	CM-6.C 구성 설정	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
CCCS-fPBMM-CM-6.D	CM-6.D 구성 설정	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-7.A	CM-7.A 최소 기능	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-7.A	CM-7.A 최소 기능	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-7.B	CM-7.B 최소 기능	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-7.B	CM-7.B 최소 기능	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8(1)	CM-8(1) 정보 시스템 구성 요소 인벤토리 | 설치/제거 중 업데이트	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8(1)	CM-8(1) 정보 시스템 구성 요소 인벤토리 | 설치/제거 중 업데이트	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8(2)	CM-8(2) 정보 시스템 구성 요소 인벤토리 | 자동 유지 관리	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8(2)	CM-8(2) 정보 시스템 구성 요소 인벤토리 | 자동 유지 관리	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8(3)	CM-8(3) 정보 시스템 구성 요소 인벤토리 | 자동화된 무단 구성 요소 탐지	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8(3)	CM-8(3) 정보 시스템 구성 요소 인벤토리 | 자동화된 무단 구성 요소 탐지	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-CM-8(3)	CM-8(3) 정보 시스템 구성 요소 인벤토리 | 자동화된 무단 구성 요소 탐지	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8(3)	CM-8(3) 정보 시스템 구성 요소 인벤토리 | 자동화된 무단 구성 요소 탐지	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-CM-8.A	CM-8.A 정보 시스템 구성 요소 인벤토리	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8.A	CM-8.A 정보 시스템 구성 요소 인벤토리	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8.B	CM-8.B 정보 시스템 구성 요소 인벤토리	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8.B	CM-8.B 정보 시스템 구성 요소 인벤토리	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8.C	CM-8.C 정보 시스템 구성 요소 인벤토리	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8.C	CM-8.C 정보 시스템 구성 요소 인벤토리	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8.D	CM-8.D 정보 시스템 구성 요소 인벤토리	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8.D	CM-8.D 정보 시스템 구성 요소 인벤토리	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8.E	CM-8.E 정보 시스템 구성 요소 인벤토리	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CM-8.E	CM-8.E 정보 시스템 구성 요소 인벤토리	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(5)	CP-2(5) 비상 계획 | 필수 임무/비즈니스 기능 계속	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(6)	CP-2(6) 비상 계획 | 대체 처리/스토리지 사이트	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CCCS-fPBMM-CP-2(6)	CP-2(6) 비상 계획 | 대체 처리/스토리지 사이트	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(6)	CP-2(6) 비상 계획 | 대체 처리/스토리지 사이트	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(6)	CP-2(6) 비상 계획 | 대체 처리/스토리지 사이트	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(6)	CP-2(6) 비상 계획 | 대체 처리/스토리지 사이트	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2(6)	CP-2(6) 비상 계획 | 대체 처리/스토리지 사이트	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.A	CP-2.A 비상 계획	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CCCS-fPBMM-CP-2.A	CP-2.A 비상 계획	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.A	CP-2.A 비상 계획	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CCCS-fPBMM-CP-2.A	CP-2.A 비상 계획	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.A	CP-2.A 비상 계획	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
CCCS-fPBMM-CP-2.A	CP-2.A 비상 계획	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.A	CP-2.A 비상 계획	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.A	CP-2.A 비상 계획	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.B	CP-2.B 비상 계획	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CCCS-fPBMM-CP-2.B	CP-2.B 비상 계획	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.B	CP-2.B 비상 계획	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CCCS-fPBMM-CP-2.B	CP-2.B 비상 계획	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.B	CP-2.B 비상 계획	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
CCCS-fPBMM-CP-2.B	CP-2.B 비상 계획	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.B	CP-2.B 비상 계획	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.B	CP-2.B 비상 계획	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.C	CP-2.C 비상 계획	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CCCS-fPBMM-CP-2.C	CP-2.C 비상 계획	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.C	CP-2.C 비상 계획	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CCCS-fPBMM-CP-2.C	CP-2.C 비상 계획	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.C	CP-2.C 비상 계획	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
CCCS-fPBMM-CP-2.C	CP-2.C 비상 계획	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.C	CP-2.C 비상 계획	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.C	CP-2.C 비상 계획	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.D	CP-2.D 비상 계획	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CCCS-fPBMM-CP-2.D	CP-2.D 비상 계획	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.D	CP-2.D 비상 계획	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CCCS-fPBMM-CP-2.D	CP-2.D 비상 계획	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.D	CP-2.D 비상 계획	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
CCCS-fPBMM-CP-2.D	CP-2.D 비상 계획	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.D	CP-2.D 비상 계획	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.D	CP-2.D 비상 계획	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.E	CP-2.E 비상 계획	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CCCS-fPBMM-CP-2.E	CP-2.E 비상 계획	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.E	CP-2.E 비상 계획	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CCCS-fPBMM-CP-2.E	CP-2.E 비상 계획	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.E	CP-2.E 비상 계획	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
CCCS-fPBMM-CP-2.E	CP-2.E 비상 계획	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.E	CP-2.E 비상 계획	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.E	CP-2.E 비상 계획	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.F	CP-2.F 비상 계획	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CCCS-fPBMM-CP-2.F	CP-2.F 비상 계획	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.F	CP-2.F 비상 계획	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CCCS-fPBMM-CP-2.F	CP-2.F 비상 계획	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.F	CP-2.F 비상 계획	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
CCCS-fPBMM-CP-2.F	CP-2.F 비상 계획	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.F	CP-2.F 비상 계획	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.F	CP-2.F 비상 계획	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.G	CP-2.G 비상 계획	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CCCS-fPBMM-CP-2.G	CP-2.G 비상 계획	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.G	CP-2.G 비상 계획	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CCCS-fPBMM-CP-2.G	CP-2.G 비상 계획	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.G	CP-2.G 비상 계획	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
CCCS-fPBMM-CP-2.G	CP-2.G 비상 계획	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.G	CP-2.G 비상 계획	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-2.G	CP-2.G 비상 계획	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CCCS-fPBMM-CP-6(1)	CP-6(1) 대체 스토리지 사이트 | 기본 사이트와 분리	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CCCS-fPBMM-CP-6(2)	CP-6(2) 대체 스토리지 사이트 | 복구 시간/복구 시점 목표	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CCCS-fPBMM-CP-6.A	CP-6.A 대체 스토리지 사이트	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CCCS-fPBMM-CP-6.B	CP-6.B 대체 스토리지 사이트	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9(3)	CP-9(3) 정보 시스템 백업 | 중요 정보를 위한 별도의 스토리지	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
CCCS-fPBMM-CP-9(7)	CP-9(7) 정보 시스템 백업 | 이중 인증	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9(7)	CP-9(7) 정보 시스템 백업 | 이중 인증	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CCCS-fPBMM-CP-9.A	CP-9.A 정보 시스템 백업	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CCCS-fPBMM-CP-9.AA	CP-9.AA 정보 시스템 백업	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CCCS-fPBMM-CP-9.B	CP-9.B 정보 시스템 백업	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CCCS-fPBMM-CP-9.C	CP-9.C 정보 시스템 백업	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CCCS-fPBMM-CP-9.D	CP-9.D 정보 시스템 백업	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-CP-10.A	CP-10.A 정보 시스템 복구 및 재구성	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-2(1)	IA-2 (1) 식별 및 인증 (조직 사용자) | 권한이 있는 계정에 대한 네트워크 액세스	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
CCCS-fPBMM-IA-2(1)	IA-2 (1) 식별 및 인증 (조직 사용자) | 권한이 있는 계정에 대한 네트워크 액세스	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-2(1)	IA-2 (1) 식별 및 인증 (조직 사용자) | 권한이 있는 계정에 대한 네트워크 액세스	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CCCS-fPBMM-IA-2(3)	IA-2(3) 식별 및 인증 (조직 사용자) | 권한이 있는 계정에 대한 네트워크 액세스	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-2(3)	IA-2(3) 식별 및 인증 (조직 사용자) | 권한이 있는 계정에 대한 네트워크 액세스	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-2(3)	IA-2(3) 식별 및 인증 (조직 사용자) | 권한이 있는 계정에 대한 네트워크 액세스	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CCCS-fPBMM-IA-2(8)	IA-2(8) 식별 및 인증 (조직 사용자) | 권한이 있는 계정에 대한 네트워크 액세스 - 재실행 방지	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-2(8)	IA-2(8) 식별 및 인증 (조직 사용자) | 권한이 있는 계정에 대한 네트워크 액세스 - 재실행 방지	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-2(8)	IA-2(8) 식별 및 인증(조직 사용자) | 권한이 있는 계정에 대한 네트워크 액세스 - 재실행 방지	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CCCS-fPBMM-IA-2(11)	IA-2(11) 식별 및 인증(조직 사용자) | 원격 액세스 - 별도의 디바이스	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-2(11)	IA-2(11) 식별 및 인증(조직 사용자) | 원격 액세스 - 별도의 디바이스	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-2(11)	IA-2(11) 식별 및 인증(조직 사용자) | 원격 액세스 - 별도의 디바이스	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-2.A	IA-2.A 식별 및 인증(조직 사용자)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-2.A	IA-2.A 식별 및 인증(조직 사용자)	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-2.A	IA-2.A 식별 및 인증(조직 사용자)	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-2.A	IA-2.A 식별 및 인증(조직 사용자)	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CCCS-fPBMM-IA-4(4)	IA-4(4) 식별자 관리 | 사용자 상태 식별	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-4.A	IA-4.A 식별자 관리	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-4.A	IA-4.A 식별자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-4.A	IA-4.A 식별자 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-4.B	IA-4.B 식별자 관리	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-4.B	IA-4.B 식별자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-4.B	IA-4.B 식별자 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-4.C	IA-4.C 식별자 관리	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-4.C	IA-4.C 식별자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-4.C	IA-4.C 식별자 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-4.D	IA-4.D 식별자 관리	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-4.D	IA-4.D 식별자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-4.D	IA-4.D 식별자 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-4.E	IA-4.E 식별자 관리	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-4.E	IA-4.E 식별자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-4.E	IA-4.E 식별자 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5(1)	IA-5(1) 인증자 관리 | 암호 기반 인증	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5(2)	IA-5(2) 인증자 관리 | PKI 기반 인증	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
CCCS-fPBMM-IA-5(2)	IA-5(2) 인증자 관리 | PKI 기반 인증	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5(4)	IA-5(4) 인증자 관리 | 암호 강도 결정 자동 지원	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5(8)	IA-5(8) 인증자 관리 | 다중 정보 시스템 계정	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
CCCS-fPBMM-IA-5(8)	IA-5(8) 인증자 관리 | 다중 정보 시스템 계정	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5(8)	IA-5(8) 인증자 관리 | 다중 정보 시스템 계정	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.A	IA-5.A 인증자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5.A	IA-5.A 인증자 관리	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.A	IA-5.A 인증자 관리	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.A	IA-5.A 인증자 관리	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.B	IA-5.B 인증자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5.B	IA-5.B 인증자 관리	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.B	IA-5.B 인증자 관리	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.B	IA-5.B 인증자 관리	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.C	IA-5.C 인증자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5.C	IA-5.C 인증자 관리	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.C	IA-5.C 인증자 관리	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.C	IA-5.C 인증자 관리	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.D	IA-5.D 인증자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5.D	IA-5.D 인증자 관리	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.D	IA-5.D 인증자 관리	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.D	IA-5.D 인증자 관리	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.E	IA-5.E 인증자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5.E	IA-5.E 인증자 관리	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.E	IA-5.E 인증자 관리	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.E	IA-5.E 인증자 관리	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.F	IA-5.F 인증자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5.F	IA-5.F 인증자 관리	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.F	IA-5.F 인증자 관리	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.F	IA-5.F 인증자 관리	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.G	IA-5.G 인증자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5.G	IA-5.G 인증자 관리	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.G	IA-5.G 인증자 관리	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.G	IA-5.G 인증자 관리	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.H	IA-5.H 인증자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5.H	IA-5.H 인증자 관리	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.H	IA-5.H 인증자 관리	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.H	IA-5.H 인증자 관리	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.I	IA-5.I 인증자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5.I	IA-5.I 인증자 관리	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.I	IA-5.I 인증자 관리	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.I	IA-5.I 인증자 관리	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.J	IA-5.J 인증자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
CCCS-fPBMM-IA-5.J	IA-5.J 인증자 관리	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.J	IA-5.J 인증자 관리	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-IA-5.J	IA-5.J 인증자 관리	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CCCS-fPBMM-IR-6(1)	IR-6(1) 인시던트 보고 | 자동 보고	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MA-3.A	MA-3.A 유지 관리 도구	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
CCCS-fPBMM-MA-3.A	MA-3.A 유지 관리 도구	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MA-4(1)	MA-4(1) 비로컬 유지 관리 | 감사 및 검토	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
CCCS-fPBMM-MA-4(1)	MA-4(1) 비로컬 유지 관리 | 감사 및 검토	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
CCCS-fPBMM-MA-4(1)	MA-4(1) 비로컬 유지 관리 | 감사 및 검토	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MA-4(1)	MA-4(1) 비로컬 유지 관리 | 감사 및 검토	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CCCS-fPBMM-MA-4(1)	MA-4(1) 비로컬 유지 관리 | 감사 및 검토	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MA-4(1)	MA-4(1) 비로컬 유지 관리 | 감사 및 검토	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MA-4(1)	MA-4(1) 비로컬 유지 관리 | 감사 및 검토	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MA-4(1)	MA-4(1) 비로컬 유지 관리 | 감사 및 검토	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MA-4(1)	MA-4(1) 비로컬 유지 관리 | 감사 및 검토	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CCCS-fPBMM-MA-4(1)	MA-4(1) 비로컬 유지 관리 | 감사 및 검토	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MA-4(1)	MA-4(1) 비로컬 유지 관리 | 감사 및 검토	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-MP-2.A	MP-2.A 미디어 액세스	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-RA-5.A	RA-5.A 취약성 스캔	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-RA-5.B	RA-5.B 취약성 스캔	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-RA-5.C	RA-5.C 취약성 스캔	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-RA-5.D	RA-5.D 취약성 스캔	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-RA-5.E	RA-5.E 취약성 스캔	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SA-10(1)	SA-10(1) 개발자 구성 관리 | 소프트웨어/펌웨어 무결성 검증	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-5.A	SC-5.A 서비스 거부 보호	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.
CCCS-fPBMM-SC-5.A	SC-5.A 서비스 거부 보호	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-6.A	SC-6.A 리소스 가용성	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-6.A	SC-6.A 리소스 가용성	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CCCS-fPBMM-SC-6.A	SC-6.A 리소스 가용성	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-6.A	SC-6.A 리소스 가용성	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-6.A	SC-6.A 리소스 가용성	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-6.A	SC-6.A 리소스 가용성	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-6.A	SC-6.A 리소스 가용성	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-6.A	SC-6.A 리소스 가용성	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(3)	SC-7(3) 경계 보호 | 액세스 포인트	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(4)	SC-7(4) 경계 보호 | 외부 통신 서비스	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(5)	SC-7(5) 경계 보호 | 기본 거부/예외별 허용	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(5)	SC-7(5) 경계 보호 | 기본 거부/예외별 허용	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(5)	SC-7(5) 경계 보호 | 기본 거부/예외별 허용	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(5)	SC-7(5) 경계 보호 | 기본 거부/예외별 허용	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-SC-7(7)	SC-7(7) 경계 보호 | 원격 디바이스의 분할 터널링 방지	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.A	SC-7.A 경계 보호	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.B	SC-7.B 경계 보호	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-7.C	SC-7.C 경계 보호	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CCCS-fPBMM-SC-8(1)	SC-8(1) 전송 기밀성 및 무결성 | 암호화 또는 대체 물리적 보호	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-8(1)	SC-8(1) 전송 기밀성 및 무결성 | 암호화 또는 대체 물리적 보호	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
CCCS-fPBMM-SC-8(1)	SC-8(1) 전송 기밀성 및 무결성 | 암호화 또는 대체 물리적 보호	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-8(1)	SC-8(1) 전송 기밀성 및 무결성 | 암호화 또는 대체 물리적 보호	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-8(1)	SC-8(1) 전송 기밀성 및 무결성 | 암호화 또는 대체 물리적 보호	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-8(1)	SC-8(1) 전송 기밀성 및 무결성 | 암호화 또는 대체 물리적 보호	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-8(1)	SC-8(1) 전송 기밀성 및 무결성 | 암호화 또는 대체 물리적 보호	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-8(1)	SC-8(1) 전송 기밀성 및 무결성 | 암호화 또는 대체 물리적 보호	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-8(1)	SC-8(1) 전송 기밀성 및 무결성 | 암호화 또는 대체 물리적 보호	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-8.A	SC-8.A 전송 기밀성 및 무결성	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-8.A	SC-8.A 전송 기밀성 및 무결성	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-8.A	SC-8.A 전송 기밀성 및 무결성	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-8.A	SC-8.A 전송 기밀성 및 무결성	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-8.A	SC-8.A 전송 기밀성 및 무결성	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-8.A	SC-8.A 전송 기밀성 및 무결성	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-8.A	SC-8.A 전송 기밀성 및 무결성	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-8.A	SC-8.A 전송 기밀성 및 무결성	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-8.A	SC-8.A 전송 기밀성 및 무결성	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-12(1)	SC-12(1) 암호화 키 설정 및 관리 | 가용성	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
CCCS-fPBMM-SC-12(2)	SC-12(2) 암호화 키 설정 및 관리 | 대칭 키	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-12(2)	SC-12(2) 암호화 키 설정 및 관리 | 대칭 키	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
CCCS-fPBMM-SC-12.A	SC-12.A 암호화 키 설정 및 관리	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-12.A	SC-12.A 암호화 키 설정 및 관리	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-13.A	SC-13.A 암호화 보호	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-22.A	SC-22.A 이름/주소 확인 서비스를 위한 아키텍처 및 프로비저닝	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CCCS-fPBMM-SC-23.A	SC-23.A 세션 인증	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-23.A	SC-23.A 세션 인증	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-23.A	SC-23.A 세션 인증	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-23.A	SC-23.A 세션 인증	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-23.A	SC-23.A 세션 인증	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-23.A	SC-23.A 세션 인증	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-23.A	SC-23.A 세션 인증	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-23.A	SC-23.A 세션 인증	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-23.A	SC-23.A 세션 인증	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28(1)	SC-28(1) 저장된 정보 보호 | 암호화 보호	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CCCS-fPBMM-SC-28.A	SC-28.A 저장된 정보 보호	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2(2)	SI-2(2) 결함 수정 | 자동 결함 수정 상태	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2(3)	SI-2(3) 결함 수정 | 결함 수정 시간/시정 조치 벤치마크	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.A	SI-2.A 결함 수정	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.B	SI-2.B 결함 수정	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.C	SI-2.C 결함 수정	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 향상된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-2.D	SI-2.D 결함 수정	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-3(1)	SI-3(1) 악성 코드 보호 | 중앙 관리	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-3(7)	SI-3(7) 악성 코드 보호 | 비서명 기반 탐지	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-3.A	SI-3.A 악성 코드 보호	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-3.A	SI-3.A 악성 코드 보호	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-3.A	SI-3.A 악성 코드 보호	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-SI-3.A	SI-3.A 악성 코드 보호	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-3.A	SI-3.A 악성 코드 보호	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-3.B	SI-3.B 악성 코드 보호	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-3.B	SI-3.B 악성 코드 보호	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-SI-3.B	SI-3.B 악성 코드 보호	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-3.B	SI-3.B 악성 코드 보호	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-3.C	SI-3.C 악성 코드 보호	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-3.C	SI-3.C 악성 코드 보호	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-SI-3.C	SI-3.C 악성 코드 보호	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-3.C	SI-3.C 악성 코드 보호	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-3.D	SI-3.D 악성 코드 보호	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-3.D	SI-3.D 악성 코드 보호	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CCCS-fPBMM-SI-3.D	SI-3.D 악성 코드 보호	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-3.D	SI-3.D 악성 코드 보호	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-4(1)	SI-4(1) 정보 시스템 모니터링 | 시스템 전반의 침입 탐지 시스템	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4(1)	SI-4(1) 정보 시스템 모니터링 | 시스템 전반의 침입 탐지 시스템	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4(2)	SI-4(2) 정보 시스템 모니터링 | 실시간 분석을 위한 자동화 도구	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4(2)	SI-4(2) 정보 시스템 모니터링 | 실시간 분석을 위한 자동화 도구	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4(4)	SI-4(4) 정보 시스템 모니터링 | 인바운드 및 아웃바운드 통신 트래픽	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-4(4)	SI-4(4) 정보 시스템 모니터링 | 인바운드 및 아웃바운드 통신 트래픽	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4(5)	SI-4(5) 정보 시스템 모니터링 | 시스템 생성 경보	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4(11)	SI-4(11) 정보 시스템 모니터링 | 통신 트래픽 이상 항목 분석	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4(11)	SI-4(11) 정보 시스템 모니터링 | 통신 트래픽 이상 항목 분석	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4(16)	SI-4(16) 정보 시스템 모니터링 | 모니터링 정보 상관 관계 분석	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4(16)	SI-4(16) 정보 시스템 모니터링 | 모니터링 정보 상관 관계 분석	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4(20)	SI-4(20) 정보 시스템 모니터링 | 권한이 있는 사용자	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CCCS-fPBMM-SI-4(23)	SI-4(23) 정보 시스템 모니터링 | 호스트 기반 디바이스	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4(23)	SI-4(23) 정보 시스템 모니터링 | 호스트 기반 디바이스	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.A	SI-4.A 정보 시스템 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.A	SI-4.A 정보 시스템 모니터링	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.A	SI-4.A 정보 시스템 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-4.A	SI-4.A 정보 시스템 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.A	SI-4.A 정보 시스템 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.B	SI-4.B 정보 시스템 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.B	SI-4.B 정보 시스템 모니터링	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.B	SI-4.B 정보 시스템 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-4.B	SI-4.B 정보 시스템 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.B	SI-4.B 정보 시스템 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.C	SI-4.C 정보 시스템 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.C	SI-4.C 정보 시스템 모니터링	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.C	SI-4.C 정보 시스템 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-4.C	SI-4.C 정보 시스템 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.C	SI-4.C 정보 시스템 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.D	SI-4.D 정보 시스템 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.D	SI-4.D 정보 시스템 모니터링	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.D	SI-4.D 정보 시스템 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-4.D	SI-4.D 정보 시스템 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.D	SI-4.D 정보 시스템 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.E	SI-4.E 정보 시스템 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.E	SI-4.E 정보 시스템 모니터링	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.E	SI-4.E 정보 시스템 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-4.E	SI-4.E 정보 시스템 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.E	SI-4.E 정보 시스템 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.F	SI-4.F 정보 시스템 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.F	SI-4.F 정보 시스템 모니터링	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.F	SI-4.F 정보 시스템 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-4.F	SI-4.F 정보 시스템 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.F	SI-4.F 정보 시스템 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.G	SI-4.G 정보 시스템 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.G	SI-4.G 정보 시스템 모니터링	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.G	SI-4.G 정보 시스템 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-4.G	SI-4.G 정보 시스템 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-4.G	SI-4.G 정보 시스템 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-5.A	SI-5.A 보안 경고, 권고 및 지침	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-5.B	SI-5.B 보안 경고, 권고 및 지침	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-5.C	SI-5.C 보안 경고, 권고 및 지침	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CCCS-fPBMM-SI-5.D	SI-5.D 보안 경고, 권고 및 지침	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-7(1)	SI-7(1) 소프트웨어, 펌웨어 및 정보 무결성 | 무결성 검사	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-7(7)	SI-7(7) 소프트웨어, 펌웨어 및 정보 무결성 | 탐지 및 대응 통합	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CCCS-fPBMM-SI-7.A	SI-7.A 소프트웨어, 펌웨어 및 정보 무결성	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
CCCS-fPBMM-SI-12.A	SI-12.A 정보 처리 및 보존	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

템플릿

템플릿은 GitHub: Operational Best Practices for Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile에서 확인할 수 있습니다.

CIS AWS 파운데이션 벤치마크 v1.4 레벨 1 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 CIS(인터넷 보안 센터) Amazon Web Services Foundation v1.4 레벨 1과 AWS 관리형 Config 규칙/AWS Config 프로세스 검사 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 CIS Amazon Web Services Foundation v1.4 레벨 1 제어와 관련이 있습니다. CIS Amazon Web Services Foundation v1.4 레벨 1 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

프로세스 확인에 관한 자세한 내용은 process-checks를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.1	현재 연락처 세부 정보 유지	account-contact-details-configured(프로세스 확인)	AWS 계정의 연락처 이메일과 전화 번호가 최신 정보에 해당되며 조직 내 두 명 이상의 개인에게 매핑되는지 확인합니다. 콘솔의 내 계정 섹션에서 연락처 정보 섹션에 올바른 정보가 지정되어 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전

제어 ID	제어 설명	AWS 구성 규칙	지침
			1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
1.2	보안 연락처 정보가 등록되는지 확인	account-security-contact-configured(프로세스 확인)	조직 보안팀의 연락처 이메일과 전화번호가 최신 정보인지 확인합니다. AWS 관리 콘솔의 내 계정 섹션에서 보안 섹션에 올바른 정보가 지정되어 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4	'루트' 사용자 액세스 키가 없는지 확인하세요.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
1.5	'루트' 사용자에 대해 MFA가 활성화되었는지 확인	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.7	관리 및 일상 작업에 '루트' 사용자를 사용하지 않아도 됩니다.	root-account-regular-use(프로세스 확인)	일상적인 작업에 루트 계정을 사용하지 않도록 하세요. IAM 내에서 보안 인증 보고서를 실행하여 루트 사용자를 마지막으로 사용한 시기를 조사하세요. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.8	IAM 암호 정책에서 최소한 14자 이상을 요구하는지 확인	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.9	IAM 암호 정책에서 암호 재사용 방지하는지 확인	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
1.10	콘솔 암호가 있는 모든 사용자에 대해 다중 인증(MFA)이 활성화되었는지 확인	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.11	콘솔 암호가 있는 모든 사용자에 대해 초기 사용자 설정 중 액세스 키를 설정해서는 안 됨	iam-user-console-and-api-access-at-creation(프로세스 확인)	콘솔 암호가 있는 모든 사용자에 대해 초기 사용자 설정 중 액세스 키가 설정되지 않았는지 확인합니다. 콘솔 액세스 권한이 있는 모든 사용자에 대해 사용자의 '생성 시간'을 액세스 키 '생성' 날짜와 비교하세요. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.12	45일 이상 사용하지 않은 보안 인증이 비활성화되어 있는지 확인	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증이 발견되면 최소 권한의 원칙에 위배될 수 있으므로 보안 인증을 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(CIS 표준 값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.13	단일 사용자가 사용할 수 있는 활성 액세스 키가 단 하나뿐인지 확인	iam-user-single-access-key(프로세스 확인)	단일 사용자가 사용할 수 있는 활성 액세스 키가 단 하나뿐인지 확인하세요. 모든 사용자에 대해서는 IAM 내 각 사용자에 대한 보안 자격 증명 탭 내에서 활성 키가 하나만 사용되는지 확인하세요. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.14	90일 또는 그보다 짧은 주기마다 액세스 키가 교체되는지 확인	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
1.15	사용자가 그룹을 통해서만 권한을 받는지 확인	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.15	사용자가 그룹을 통해서만 권한을 받는지 확인	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
1.15	사용자가 그룹을 통해서만 권한을 받는지 확인	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.16	전체 '*:*' 관리자 권한을 허용하는 IAM 정책이 연결되지 않도록 되어 있는지 확인	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리의 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.17	Support를 사용하여 인시던트를 관리하기 위한 AWS 지원 역할이 생성되었는지 확인합니다.	iam-policy-in-use	AWS Identity and Access Management(IAM)는 IAM 정책이 적절한 사용자, 역할 또는 그룹에 할당되도록 하여 액세스 권한 및 권한 부여를 관리하는 데 도움이 될 수 있습니다. 이러한 정책을 제한하는 것은 최소 권한 및 업무 분리의 원칙도 포함합니다. 이 규칙을 사용하려면 AWS Support를 통한 인시던트 관리를 위해 policyARN을 arn:aws:iam::aws:policy/AWSSupportAccess로 설정해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.19	AWS IAM에 저장된 만료된 SSL/TLS 인증서가 모두 제거되었는지 확인	iam-expired-certificates(프로세스 확인)	IAM에 저장된 만료된 SSL/TLS 인증서가 모두 제거되었는지 확인합니다. CLI가 설치된 명령줄에서 'AWS iam list-server-certificates' 명령을 AWS 실행하고 만료된 서버 인증서가 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.20	AWS IAM Access Analyzer가 활성화되어 있는지 확인	iam-access-analyzer-enabled(프로세스 확인)	IAM Access Analyzer가 활성화되어 있는지 확인합니다. 콘솔의 IAM 섹션 내에서 Access Analyzer를 선택하고 상태가 활성으로 설정되어 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1.3	S3 버킷에서 MFA 삭제가 활성화되어 있는지 확인	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 버전을 유지할 수 있습니다. S3 버킷에 다중 인증(MFA) 삭제를 추가할 때 버킷의 버전 상태를 변경하거나 객체 버전을 삭제하려면 추가 인증 요소가 필요합니다. 보안 자격 증명이 손상되거나 무단 액세스가 허용될 경우, MFA 삭제는 보안 계층을 한층 더 보강할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1.5	S3 버킷이 '퍼블릭 액세스 차단(버킷 설정)'으로 구성되어 있는지 확인	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1.5	S3 버킷이 '퍼블릭 액세스 차단(버킷 설정)'으로 구성되어 있는지 확인	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
2.2.1	EBS 볼륨 암호화가 활성화되어 있는지 확인	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.1	EBS 볼륨 암호화가 활성화되어 있는지 확인	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.3.1	RDS 인스턴스에 암호화가 활성화되어 있는지 확인하세요.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.3.1	RDS 인스턴스에 암호화가 활성화되어 있는지 확인하세요.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1	모든 리전에서 CloudTrail이 활성화되어 있는지 확인	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	CloudTrail 로그를 저장하는 데 사용된 S3 버킷에 대한 퍼블릭 액세스가 불가능하도록 되어 있는지 확인	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.3	CloudTrail 로그를 저장하는 데 사용된 S3 버킷에 대한 퍼블릭 액세스가 불가능하도록 되어 있는지 확인	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	CloudTrail 로그를 저장하는 데 사용된 S3 버킷에 대한 퍼블릭 액세스가 불가능하도록 되어 있는지 확인	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
3.4	CloudTrail 추적이 CloudWatch Logs와 통합되었는지 확인	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6	CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	무단 API 직접 호출에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-unauthorized-api-calls(프로세스 확인)	무단 API 직접 호출에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.2	MFA 없는 Management Console 로그인에 대해 로그 지표 필터 및 경보가 존재하는지 확인	alarm-sign-in-without-mfa(프로세스 확인)	다중 인증(MFA)을 사용하지 않는 AWS Management Console 로그인에 대한 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.3	'루트' 계정 사용에 대해 로그 지표 필터 및 경보가 존재하는지 확인	alarm-root-account-use(프로세스 확인)	루트 계정 사용에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.4	IAM 정책 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-iam-policy-change(프로세스 확인)	IAM 정책 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.5	구성 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-cloudtrail-config-change(프로세스 확인)	AWS CloudTrail 구성 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.8	S3 버킷 정책 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-s3-bucket-policy-change(프로세스 확인)	Amazon S3 버킷 정책 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.12	네트워크 게이트웨이 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-vpc-network-gateway-change(프로세스 확인)	네트워크 게이트웨이 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.13	라우팅 테이블 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-vpc-route-table-change(프로세스 확인)	라우팅 테이블 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.14	VPC 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-vpc-change(프로세스 확인)	Amazon Virtual Private Cloud(VPC) 변경에 대한 로그 지표 필터와 경보가 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.15	AWS Organizations 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-organizations-change(프로세스 확인)	AWS Organizations 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.1	0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하는 네트워크 ACL이 없는지 확인	nacl-no-unrestricted-ssh-rdp	원격 서버 관리 포트로의 공개 수신을 허용하는 네트워크 ACL이 없는지 확인합니다. 콘솔의 VPC 섹션 내에서 원격 서버 관리 포트를 포함해 허용하는 포트 또는 포트 범위가 있으면서 소스가 '0.0.0.0/0'인 네트워크 ACL이 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하는 보안 그룹은 없는지 확인	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하는 보안 그룹은 없는지 확인	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터(CIS 표준 값: 3389)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

템플릿

템플릿은 GitHub: CIS AWS Foundations 벤치마크 v1.4 레벨 1의 운영 모범 사례에서 사용할 수 있습니다.

CIS AWS 파운데이션 벤치마크 v1.4 레벨 2 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 CIS(인터넷 보안 센터) Amazon Web Services Foundation v1.4 레벨 2와 AWS 관리형 Config 규칙/AWS Config 프로세스 검사 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 CIS Amazon Web Services Foundation v1.4 레벨 2 제어와 관련이 있습니다. CIS Amazon Web Services Foundation v1.4 레벨 2 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

프로세스 확인에 관한 자세한 내용은 process-checks를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.1	현재 연락처 세부 정보 유지	account-contact-details-configured(프로세스 확인)	AWS 계정의 연락처 이메일과 전화 번호가 최신 정보에 해당되며 조직 내 두 명 이상의 개인에게 매핑되는지 확인합니다. 콘솔의 내 계정 섹션에서 연락처 정보 섹션에 올바른 정보가 지정되어 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
1.2	보안 연락처 정보가 등록되는지 확인	account-security-contact-configured(프로세스 확인)	조직 보안팀의 연락처 이메일과 전화번호가 최신 정보인지 확인합니다. AWS 관리 콘솔의 내 계정 섹션

제어 ID	제어 설명	AWS 구성 규칙	지침
			에서 보안 섹션에 올바른 정보가 지정되어 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
1.4	'루트' 사용자 액세스 키가 없는지 확인하세요.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5	'루트' 사용자에 대해 MFA가 활성화되었는지 확인	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
1.6	'루트' 사용자 계정에 대해 하드웨어 MFA가 활성화되어 있는지 확인	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.7	관리 및 일상 작업에 '루트' 사용자를 사용하지 않아도 됩니다.	root-account-regular-use(프로세스 확인)	일상적인 작업에 루트 계정을 사용하지 않도록 하세요. IAM 내에서 보안 인증 보고서를 실행하여 루트 사용자를 마지막으로 사용한 시기를 조사하세요. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.8	IAM 암호 정책에서 최소한 14자 이상을 요구하는지 확인	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.9	IAM 암호 정책에서 암호 재사용 방지하는지 확인	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
1.10	콘솔 암호가 있는 모든 사용자에 대해 다중 인증(MFA)이 활성화되었는지 확인	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.11	콘솔 암호가 있는 모든 사용자에 대해 초기 사용자 설정 중 액세스 키를 설정해서는 안 됨	iam-user-console-and-api-access-at-creation(프로세스 확인)	콘솔 암호가 있는 모든 사용자에 대해 초기 사용자 설정 중 액세스 키가 설정되지 않았는지 확인합니다. 콘솔 액세스 권한이 있는 모든 사용자에 대해 사용자의 '생성 시간'을 액세스 키 '생성' 날짜와 비교하세요. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.12	45일 이상 사용하지 않은 보안 인증이 비활성화되어 있는지 확인	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증이 발견되면 최소 권한의 원칙에 위배될 수 있으므로 보안 인증을 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(CIS 표준 값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.13	단일 사용자가 사용할 수 있는 활성 액세스 키가 단 하나뿐인지 확인	iam-user-single-access-key(프로세스 확인)	단일 사용자가 사용할 수 있는 활성 액세스 키가 단 하나뿐인지 확인하세요. 모든 사용자에 대해서는 IAM 내 각 사용자에 대한 보안 자격 증명 탭 내에서 활성 키가 하나만 사용되는지 확인하세요. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.14	90일 또는 그보다 짧은 주기마다 액세스 키가 교체되는지 확인	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
1.15	사용자가 그룹을 통해서만 권한을 받는지 확인	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.15	사용자가 그룹을 통해서만 권한을 받는지 확인	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
1.15	사용자가 그룹을 통해서만 권한을 받는지 확인	iam-user-group-membership-check	AWS Identity and Access Managemen t(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.16	전체 '*:*' 관리자 권한을 허용하는 IAM 정책이 연결되지 않도록 되어 있는지 확인	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리의 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.17	Support를 사용하여 인시던트를 관리하기 위한 AWS 지원 역할이 생성되었는지 확인합니다.	iam-policy-in-use	AWS Identity and Access Managemen t(IAM)는 IAM 정책이 적절한 사용자, 역할 또는 그룹에 할당되도록 하여 액세스 권한 및 권한 부여를 관리하는 데 도움이 될 수 있습니다. 이러한 정책을 제한하는 것은 최소 권한 및 업무 분리의 원칙도 포함합니다. 이 규칙을 사용하려면 AWS Support를 통한 인시던트 관리를 위해 policyARN을 arn:aws:iam::aws:policy/AWS SupportAccess로 설정해야 합니다.
1.18	IAM 인스턴스 역할이 인스턴스의 AWS 리소스 액세스에 사용되는지 확인	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.19	AWS IAM에 저장된 만료된 SSL/TLS 인증서가 모두 제거되었는지 확인	iam-expired-certificates(프로세스 확인)	IAM에 저장된 만료된 SSL/TLS 인증서가 모두 제거되었는지 확인합니다. AWS CLI가 설치된 명령줄에서 'AWS iam list-server-certificates' 명령을 실행하고 만료된 서버 인증서가 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.20	AWS IAM Access Analyzer가 활성화되어 있는지 확인	iam-access-analyzer-enabled(프로세스 확인)	IAM Access Analyzer가 활성화되어 있는지 확인합니다. 콘솔의 IAM 섹션 내에서 Access Analyzer를 선택하고 상태가 활성으로 설정되어 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
1.21	다중 계정 환경의 ID 페더레이션 또는 AWS 조직에서 사용자를 중앙에서 관리하도록 보장	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1.1	모든 S3 버킷이 저장 시 암호화를 사용하는지 확인	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
2.1.2	S3 버킷 정책이 HTTP 요청을 거부하도록 설정되어 있는지 확인	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1.3	S3 버킷에서 MFA 삭제가 활성화되어 있는지 확인	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 버전을 유지할 수 있습니다. S3 버킷에 다중 인증(MFA) 삭제를 추가할 때 버킷의 버전 상태를 변경하거나 객체 버전을 삭제하려면 추가 인증 요소가 필요합니다. 보안 자격 증명이 손상되거나 무단 액세스가 허용될 경우, MFA 삭제는 보안 계층을 한층 더 보강할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1.5	S3 버킷이 '퍼블릭 액세스 차단(버킷 설정)'으로 구성되어 있는지 확인	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1.5	S3 버킷이 '퍼블릭 액세스 차단(버킷 설정)'으로 구성되어 있는지 확인	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
2.2.1	EBS 볼륨 암호화가 활성화되어 있는지 확인	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.1	EBS 볼륨 암호화가 활성화되어 있는지 확인	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.3.1	RDS 인스턴스에 암호화가 활성화되어 있는지 확인하세요.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.3.1	RDS 인스턴스에 암호화가 활성화되어 있는지 확인하세요.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1	모든 리전에서 CloudTrail이 활성화되어 있는지 확인	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2	CloudTrail 로그 파일 검증이 활성화되어 있는지 확인	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
3.3	CloudTrail 로그를 저장하는 데 사용된 S3 버킷에 대한 퍼블릭 액세스가 불가능하도록 되어 있는지 확인	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	CloudTrail 로그를 저장하는 데 사용된 S3 버킷에 대한 퍼블릭 액세스가 불가능하도록 되어 있는지 확인	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.3	CloudTrail 로그를 저장하는 데 사용된 S3 버킷에 대한 퍼블릭 액세스가 불가능하도록 되어 있는지 확인	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	CloudTrail 추적이 CloudWatch Logs와 통합되었는지 확인	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
3.5	모든 리전에서 AWS Config가 활성화되어 있는지 확인	config-enabled-all-regions(프로세스 확인)	모든 AWS 리전에서 AWS Config가 활성화되어 있는지 확인합니다. 콘솔의 AWS Config 섹션에서 활성화된 각 리전에 대해 AWS Config 레코더가 올바르게 구성되었는지 확인합니다. 적어도 한 리전에서 글로벌 AWS 리소스 기록이 활성화되어 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6	CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
3.7	KMS CMK를 사용해 CloudTrail 로그가 저장 시 암호화되는지 확인	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
3.8	고객이 생성한 CMK 교체가 활성화되어 있는지 확인	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.9	모든 VPC에서 VPC 플로우 로깅이 활성화되어 있는지 확인	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
3.10	쓰기 이벤트에 대한 객체 수준 로깅이 S3 버킷에 대해 활성화되어 있는지 확인	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
3.11	읽기 이벤트에 대한 객체 수준 로깅이 S3 버킷에 대해 활성화되어 있는지 확인	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	무단 API 직접 호출에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-unauthorized-api-calls(프로세스 확인)	무단 API 직접 호출에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.2	MFA 없는 Management Console 로그인에 대해 로그 지표 필터 및 경보가 존재하는지 확인	alarm-sign-in-without-mfa(프로세스 확인)	다중 인증(MFA)을 사용하지 않는 AWS Management Console 로그인에 대한 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.3	'루트' 계정 사용에 대해 로그 지표 필터 및 경보가 존재하는지 확인	alarm-root-account-use(프로세스 확인)	루트 계정 사용에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.4	IAM 정책 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-iam-policy-change(프로세스 확인)	IAM 정책 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.5	구성 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-cloudtrail-config-change(프로세스 확인)	AWS CloudTrail 구성 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.6	AWS Management Console 인증 실패에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-console-auth-failures(프로세스 확인)	AWS Management Console 인증 실패에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.7	고객이 생성한 CMK의 비활성화 또는 예약된 삭제에 대해 로그 지표 필터 및 경보가 존재하는지 확인	alarm-kms-disable-or-delete-cmk(프로세스 확인)	고객이 생성한 CMK의 비활성화 또는 예약된 삭제에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.8	S3 버킷 정책 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-s3-bucket-policy-change(프로세스 확인)	Amazon S3 버킷 정책 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.9	Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는 AWS 지 확인	alarm-aws-config-change(프로세스 확인)	AWS Config 구성 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.10	보안 그룹 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-vpc-secrity-group-change(프로세스 확인)	보안 그룹 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.11	네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-vpc-nacl-change(프로세스 확인)	네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.12	네트워크 게이트웨이 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-vpc-network-gateway-change(프로세스 확인)	네트워크 게이트웨이 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.13	라우팅 테이블 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-vpc-route-table-change(프로세스 확인)	라우팅 테이블 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.
4.14	VPC 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-vpc-change(프로세스 확인)	Amazon Virtual Private Cloud(VPC) 변경에 대한 로그 지표 필터와 경보가 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.15	AWS Organizations 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인	alarm-organizations-change(프로세스 확인)	AWS Organizations 변경 사항에 대해 로그 지표 필터와 경보가 존재하는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.1	0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하는 네트워크 ACL이 없는지 확인	nacl-no-unrestricted-ssh-rdp	원격 서버 관리 포트로의 공개 수신을 허용하는 네트워크 ACL이 없는지 확인합니다. 콘솔의 VPC 섹션 내에서 원격 서버 관리 포트를 포함해 허용하는 포트 또는 포트 범위가 있으면서 소스가 '0.0.0.0/0'인 네트워크 ACL이 있는지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하는 보안 그룹은 없는지 확인	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하는 보안 그룹은 없는지 확인	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터(CIS 표준 값: 3389)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3	모든 VPC의 기본 보안 그룹이 모든 트래픽을 제한하는지 확인	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4	VPC 피어링을 위한 라우팅 테이블이 '최소 액세스 권한'인지 여부를 확인합니다.	vpc-peering-least-access(프로세스 확인)	4.4 VPC 피어링을 위한 라우팅 테이블이 '최소 액세스 권한'인지 여부를 확인합니다. 콘솔의 VPC 섹션 내에서 라우팅 테이블 항목을 검사하여 피어링 목적을 달성하는 데 필요한 최소 수의 서브넷 또는 호스트가 라우팅 가능한지 확인합니다. 이 제어 기능의 감사에 관한 자세한 내용은 CIS Amazon Web Services Foundations Benchmark 버전 1.4.0 문서(웹사이트 https://www.cisecurity.org/benchmark/amazon_web_services/에서 확인 가능)를 참조하세요.

템플릿

템플릿은 GitHub: CIS AWS Foundations 벤치마크 v1.4 레벨 2 운영 모범 사례에서 사용할 수 있습니다.

CIS Critical Security Controls v8 IG1 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 인터넷 보안 센터(CIS) 중요 보안 제어 v8 IG1과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각는 특정 AWS 리소스에 AWS Config 적용되며 하나 이상의 CIS Critical Security Controls v8 IG1 제어와 관련이 있습니다. CIS Critical Security Controls v8 IG1 제어는 여러 AWS Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.1	상세한 기업 자산 인벤토리 수립 및 유지	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
1.1	상세한 기업 자산 인벤토리 수립 및 유지	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크

제어 ID	제어 설명	AWS 구성 규칙	지침
			액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-security-group-attached-to-eni	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	권한이 부여된 소프트웨어가 현재 지원되는지 확인	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
2.2	권한이 부여된 소프트웨어가 현재 지원되는지 확인	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	권한이 부여된 소프트웨어가 현재 지원되는지 확인	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. Fargate 플랫폼 버전에 AWS 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.
3.3	데이터 액세스 제어 목록 구성	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
3.3	데이터 액세스 제어 목록 구성	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
3.3	데이터 액세스 제어 목록 구성	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
3.3	데이터 액세스 제어 목록 구성	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.3	데이터 액세스 제어 목록 구성	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
3.3	데이터 액세스 제어 목록 구성	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
3.3	데이터 액세스 제어 목록 구성	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
3.3	데이터 액세스 제어 목록 구성	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
3.3	데이터 액세스 제어 목록 구성	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	데이터 보존 적용	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
3.4	데이터 보존 적용	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
4.1	안전한 구성 프로세스 수립 및 유지	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
4.1	안전한 구성 프로세스 수립 및 유지	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
4.1	안전한 구성 프로세스 수립 및 유지	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
4.1	안전한 구성 프로세스 수립 및 유지	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.6	기업 자산 및 소프트웨어를 안전하게 관리	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.6	기업 자산 및 소프트웨어를 안전하게 관리	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.7	기업 자산 및 소프트웨어 기본 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
5.1	계정 인벤토리 수립 및 유지	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	고유 암호 사용	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
5.2	고유 암호 사용	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	고유 암호 사용	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	고유 암호 사용	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3	휴면 계정 비활성화	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4	관리자 권한을 전용 관리자 계정으로 제한	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
5.4	관리자 권한을 전용 관리자 계정으로 제한	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 사용자가 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4	원격 네트워크 액세스에 MFA 요구	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.
6.4	원격 네트워크 액세스에 MFA 요구	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4	원격 네트워크 액세스에 MFA 요구	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
6.5	관리 액세스에 MFA 요구	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1	취약성 관리 프로세스 수립 및 유지	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1	취약성 관리 프로세스 수립 및 유지	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
7.1	취약성 관리 프로세스 수립 및 유지	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3	자동화된 운영 체제 패치 관리 수행	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
7.3	자동화된 운영 체제 패치 관리 수행	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3	자동화된 운영 체제 패치 관리 수행	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.4	자동화된 애플리케이션 패치 관리 수행	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
7.4	자동화된 애플리케이션 패치 관리 수행	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.4	자동화된 애플리케이션 패치 관리 수행	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
8.1	감사 로그 관리 프로세스 수립 및 유지	audit-log-policy-exists(프로세스 확인)	조직의 로깅 요구 사항을 정의하는 감사 로그 관리 정책을 수립하고 유지 관리합니다. 여기에는 감사 로그의 검토 및 보존이 포함되며 이에 국한되지는 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
8.2	감사 로그 수집	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
8.2	감사 로그 수집	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
8.2	감사 로그 수집	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
8.2	감사 로그 수집	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
8.2	감사 로그 수집	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
8.2	감사 로그 수집	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3	적절한 감사 로그 저장 보장	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
10.1	맬웨어 방지 소프트웨어 배포 및 유지 관리	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2	자동 맬웨어 방지 서명 업데이트 구성	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
11.2	자동 백업 수행	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.2	자동 백업 수행	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
11.2	자동 백업 수행	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.2	자동 백업 수행	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
11.2	자동 백업 수행	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
11.2	자동 백업 수행	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
11.3	복구 데이터 보호	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	복구 데이터 보호	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
11.3	복구 데이터 보호	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.3	복구 데이터 보호	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

템플릿

템플릿은 GitHub: CIS Critical Security Controls v8 IG1 운영 모범 사례에서 확인할 수 있습니다.

CIS 핵심 보안 제어 v8 IG2 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 인터넷 보안 센터(CIS) 중요 보안 제어 v8 IG2와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각는 특정 AWS 리소스에 AWS Config 적용되며 하나 이상의 CIS Critical Security Controls v8 IG2 제어와 관련이 있습니다. CIS Critical Security Controls v8 IG2 제어는 여러 AWS Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.1	상세한 기업 자산 인벤토리 수립 및 유지	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
1.1	상세한 기업 자산 인벤토리 수립 및 유지	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크

제어 ID	제어 설명	AWS 구성 규칙	지침
			액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-security-group-attached-to-eni	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	권한이 부여된 소프트웨어가 현재 지원되는지 확인	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
2.2	권한이 부여된 소프트웨어가 현재 지원되는지 확인	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	권한이 부여된 소프트웨어가 현재 지원되는지 확인	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. Fargate 플랫폼 버전에 영향을 AWS 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.4	자동 소프트웨어 인벤토리 도구 활용	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.4	자동 소프트웨어 인벤토리 도구 활용	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
3.3	데이터 액세스 제어 목록 구성	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
3.3	데이터 액세스 제어 목록 구성	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
3.3	데이터 액세스 제어 목록 구성	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
3.3	데이터 액세스 제어 목록 구성	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.3	데이터 액세스 제어 목록 구성	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
3.3	데이터 액세스 제어 목록 구성	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
3.3	데이터 액세스 제어 목록 구성	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
3.3	데이터 액세스 제어 목록 구성	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
3.3	데이터 액세스 제어 목록 구성	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	데이터 보존 적용	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
3.4	데이터 보존 적용	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
3.10	민감한 전송 중 데이터 암호화	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.10	민감한 전송 중 데이터 암호화	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.10	민감한 전송 중 데이터 암호화	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.10	민감한 전송 중 데이터 암호화	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.10	민감한 전송 중 데이터 암호화	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.10	민감한 전송 중 데이터 암호화	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.10	민감한 전송 중 데이터 암호화	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
3.10	민감한 전송 중 데이터 암호화	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.10	민감한 전송 중 데이터 암호화	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.10	민감한 전송 중 데이터 암호화	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
3.11	민감한 저장 데이터 암호화	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
3.11	민감한 저장 데이터 암호화	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
3.11	민감한 저장 데이터 암호화	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
4.1	안전한 구성 프로세스 수립 및 유지	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
4.1	안전한 구성 프로세스 수립 및 유지	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
4.1	안전한 구성 프로세스 수립 및 유지	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
4.1	안전한 구성 프로세스 수립 및 유지	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.6	기업 자산 및 소프트웨어를 안전하게 관리	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.6	기업 자산 및 소프트웨어를 안전하게 관리	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.7	기업 자산 및 소프트웨어 기본 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
5.1	계정 인벤토리 수립 및 유지	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	고유 암호 사용	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
5.2	고유 암호 사용	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	고유 암호 사용	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	고유 암호 사용	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3	휴면 계정 비활성화	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4	관리자 권한을 전용 관리자 계정으로 제한	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
5.4	관리자 권한을 전용 관리자 계정으로 제한	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.6	계정 관리를 중앙 집중화	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
6.4	원격 네트워크 액세스에 MFA 요구	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4	원격 네트워크 액세스에 MFA 요구	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4	원격 네트워크 액세스에 MFA 요구	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
6.5	관리 액세스에 MFA 요구	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.7	액세스 제어 중앙 집중화	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
7.1	취약성 관리 프로세스 수립 및 유지	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1	취약성 관리 프로세스 수립 및 유지	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
7.1	취약성 관리 프로세스 수립 및 유지	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3	자동화된 운영 체제 패치 관리 수행	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
7.3	자동화된 운영 체제 패치 관리 수행	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3	자동화된 운영 체제 패치 관리 수행	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.4	자동화된 애플리케이션 패치 관리 수행	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
7.4	자동화된 애플리케이션 패치 관리 수행	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.4	자동화된 애플리케이션 패치 관리 수행	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.5	내부 기업 자산의 취약성 자동 스캔 수행	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository(ECR) 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.
8.1	감사 로그 관리 프로세스 수립 및 유지	audit-log-policy-exists(프로세스 확인)	조직의 로깅 요구 사항을 정의하는 감사 로그 관리 정책을 수립하고 유지 관리합니다. 여기에는 감사 로그의 검토 및 보존이 포함되며 이에 국한되지는 않습니다.
8.2	감사 로그 수집	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
8.2	감사 로그 수집	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
8.2	감사 로그 수집	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
8.2	감사 로그 수집	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
8.2	감사 로그 수집	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
8.2	감사 로그 수집	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3	적절한 감사 로그 저장 보장	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
8.5	상세 감사 로그 수집	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
8.5	상세 감사 로그 수집	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
8.5	상세 감사 로그 수집	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
8.5	상세 감사 로그 수집	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
8.5	상세 감사 로그 수집	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
8.5	상세 감사 로그 수집	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
8.7	URL 요청 감사 로그 수집	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.9	감사 로그 중앙 집중화	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
8.10	감사 로그 유지	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
8.10	감사 로그 유지	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.1	맬웨어 방지 소프트웨어 배포 및 유지 관리	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
10.2	자동 맬웨어 방지 서명 업데이트 구성	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4	이동식 미디어의 자동 맬웨어 방지 검사 구성	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
10.6	맬웨어 방지 소프트웨어를 중앙에서 관리	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7	행동 기반 맬웨어 방지 소프트웨어 사용	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
11.2	자동 백업 수행	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.2	자동 백업 수행	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
11.2	자동 백업 수행	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.2	자동 백업 수행	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
11.2	자동 백업 수행	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
11.2	자동 백업 수행	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
11.3	복구 데이터 보호	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	복구 데이터 보호	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
11.3	복구 데이터 보호	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.3	복구 데이터 보호	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	elbv2-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.3	네트워크 인프라를 안전하게 관리	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
12.3	네트워크 인프라를 안전하게 관리	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.3	네트워크 인프라를 안전하게 관리	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
12.3	네트워크 인프라를 안전하게 관리	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.3	네트워크 인프라를 안전하게 관리	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
12.3	네트워크 인프라를 안전하게 관리	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.3	네트워크 인프라를 안전하게 관리	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
12.3	네트워크 인프라를 안전하게 관리	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13.1	보안 이벤트 알림 중앙 집중화	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13.1	보안 이벤트 알림 중앙 집중화	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13.3	네트워크 침입 탐지 솔루션 배포	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
13.6	네트워크 트래픽 흐름 로그 수집	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13.6	네트워크 트래픽 흐름 로그 수집	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
16.1	안전한 애플리케이션 개발 프로세스 수립 및 유지	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16.1	안전한 애플리케이션 개발 프로세스 수립 및 유지	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 보안 인증 정보가 포함되지 않도록 합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
16.1	안전한 애플리케이션 개발 프로세스 수립 및 유지	codebuild-project-environment-privileged-check	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있지 않은지 확인합니다. Docker API와 컨테이너의 기본 하드웨어에 대해 의도하지 않은 액세스를 방지하려면 이 설정을 비활성화해야 합니다.
16.1	안전한 애플리케이션 개발 프로세스 수립 및 유지	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
16.1	안전한 애플리케이션 개발 프로세스 수립 및 유지	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

템플릿

템플릿은 GitHub: Operational Best Practices for CIS Critical Security Controls v8 IG2에서 확인할 수 있습니다.

CIS 핵심 보안 제어 v8 IG3 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 인터넷 보안 센터(CIS) 중요 보안 제어 v8 IG3와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각는 특정 AWS 리소스에 AWS Config 적용되며 하나 이상의 CIS Critical Security Controls v8 IG3 제어와 관련이 있습니다. CIS Critical Security Controls v8 IG3 제어는 여러 AWS Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.1	상세한 기업 자산 인벤토리 수립 및 유지	eip-attached	이 규칙은 Amazon Virtual Private

제어 ID	제어 설명	AWS 구성 규칙	지침
			Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.1	상세한 기업 자산 인벤토리 수립 및 유지	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
1.1	상세한 기업 자산 인벤토리 수립 및 유지	ec2-security-group-attached-to-eni	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	권한이 부여된 소프트웨어가 현재 지원되는지 확인	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
2.2	권한이 부여된 소프트웨어가 현재 지원되는지 확인	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	권한이 부여된 소프트웨어가 현재 지원되는지 확인	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. Fargate 플랫폼 버전에 AWS 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.4	자동 소프트웨어 인벤토리 도구 활용	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.4	자동 소프트웨어 인벤토리 도구 활용	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
3.3	데이터 액세스 제어 목록 구성	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
3.3	데이터 액세스 제어 목록 구성	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
3.3	데이터 액세스 제어 목록 구성	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
3.3	데이터 액세스 제어 목록 구성	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.3	데이터 액세스 제어 목록 구성	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.3	데이터 액세스 제어 목록 구성	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
3.3	데이터 액세스 제어 목록 구성	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
3.3	데이터 액세스 제어 목록 구성	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
3.3	데이터 액세스 제어 목록 구성	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	데이터 액세스 제어 목록 구성	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
3.3	데이터 액세스 제어 목록 구성	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	데이터 보존 적용	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
3.4	데이터 보존 적용	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
3.10	민감한 전송 중 데이터 암호화	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.10	민감한 전송 중 데이터 암호화	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.10	민감한 전송 중 데이터 암호화	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.10	민감한 전송 중 데이터 암호화	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.10	민감한 전송 중 데이터 암호화	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.10	민감한 전송 중 데이터 암호화	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.10	민감한 전송 중 데이터 암호화	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
3.10	민감한 전송 중 데이터 암호화	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.10	민감한 전송 중 데이터 암호화	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.10	민감한 전송 중 데이터 암호화	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
3.11	민감한 저장 데이터 암호화	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
3.11	민감한 저장 데이터 암호화	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
3.11	민감한 저장 데이터 암호화	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.11	민감한 저장 데이터 암호화	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11	민감한 저장 데이터 암호화	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
3.14	민감한 데이터 액세스 로깅	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14	민감한 데이터 액세스 로깅	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14	민감한 데이터 액세스 로깅	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
3.14	민감한 데이터 액세스 로깅	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14	민감한 데이터 액세스 로깅	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
3.14	민감한 데이터 액세스 로깅	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14	민감한 데이터 액세스 로깅	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
3.14	민감한 데이터 액세스 로깅	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14	민감한 데이터 액세스 로깅	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
3.14	민감한 데이터 액세스 로깅	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14	민감한 데이터 액세스 로깅	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14	민감한 데이터 액세스 로깅	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
3.14	민감한 데이터 액세스 로깅	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14	민감한 데이터 액세스 로깅	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
4.1	안전한 구성 프로세스 수립 및 유지	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
4.1	안전한 구성 프로세스 수립 및 유지	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
4.1	안전한 구성 프로세스 수립 및 유지	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	안전한 구성 프로세스 수립 및 유지	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
4.1	안전한 구성 프로세스 수립 및 유지	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.6	기업 자산 및 소프트웨어를 안전하게 관리	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.6	기업 자산 및 소프트웨어를 안전하게 관리	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.6	기업 자산 및 소프트웨어를 안전하게 관리	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.7	기업 자산 및 소프트웨어 기본 계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
5.1	계정 인벤토리 수립 및 유지	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	고유 암호 사용	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
5.2	고유 암호 사용	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	고유 암호 사용	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	고유 암호 사용	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3	휴면 계정 비활성화	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4	관리자 권한을 전용 관리자 계정으로 제한	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
5.4	관리자 권한을 전용 관리자 계정으로 제한	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.6	계정 관리를 중앙 집중화	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
6.4	원격 네트워크 액세스에 MFA 요구	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4	원격 네트워크 액세스에 MFA 요구	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4	원격 네트워크 액세스에 MFA 요구	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
6.5	관리 액세스에 MFA 요구	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.7	액세스 제어 중앙 집중화	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
7.1	취약성 관리 프로세스 수립 및 유지	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1	취약성 관리 프로세스 수립 및 유지	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
7.1	취약성 관리 프로세스 수립 및 유지	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3	자동화된 운영 체제 패치 관리 수행	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
7.3	자동화된 운영 체제 패치 관리 수행	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3	자동화된 운영 체제 패치 관리 수행	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.4	자동화된 애플리케이션 패치 관리 수행	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
7.4	자동화된 애플리케이션 패치 관리 수행	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.4	자동화된 애플리케이션 패치 관리 수행	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.5	내부 기업 자산의 취약성 자동 스캔 수행	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository(ECR) 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.
8.1	감사 로그 관리 프로세스 수립 및 유지	audit-log-policy-exists(프로세스 확인)	조직의 로깅 요구 사항을 정의하는 감사 로그 관리 정책을 수립하고 유지 관리합니다. 여기에는 감사 로그의 검토 및 보존이 포함되며 이에 국한되지는 않습니다.
8.2	감사 로그 수집	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
8.2	감사 로그 수집	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
8.2	감사 로그 수집	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
8.2	감사 로그 수집	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
8.2	감사 로그 수집	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2	감사 로그 수집	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
8.2	감사 로그 수집	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3	적절한 감사 로그 저장 보장	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
8.5	상세 감사 로그 수집	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
8.5	상세 감사 로그 수집	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
8.5	상세 감사 로그 수집	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
8.5	상세 감사 로그 수집	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
8.5	상세 감사 로그 수집	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
8.5	상세 감사 로그 수집	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.5	상세 감사 로그 수집	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
8.7	URL 요청 감사 로그 수집	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.9	감사 로그 중앙 집중화	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
8.10	감사 로그 유지	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
8.10	감사 로그 유지	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.1	맬웨어 방지 소프트웨어 배포 및 유지 관리	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
10.2	자동 맬웨어 방지 서명 업데이트 구성	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4	이동식 미디어의 자동 맬웨어 방지 검사 구성	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
10.6	맬웨어 방지 소프트웨어를 중앙에서 관리	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7	행동 기반 맬웨어 방지 소프트웨어 사용	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
11.2	자동 백업 수행	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.2	자동 백업 수행	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
11.2	자동 백업 수행	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.2	자동 백업 수행	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
11.2	자동 백업 수행	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	자동 백업 수행	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
11.2	자동 백업 수행	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
11.3	복구 데이터 보호	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	복구 데이터 보호	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
11.3	복구 데이터 보호	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.3	복구 데이터 보호	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
11.4	복구 데이터의 격리된 인스턴스 설정 및 유지 관리	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.2	보안 네트워크 아키텍처 수립 및 유지	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
12.2	보안 네트워크 아키텍처 수립 및 유지	elbv2-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.3	네트워크 인프라를 안전하게 관리	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
12.3	네트워크 인프라를 안전하게 관리	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.3	네트워크 인프라를 안전하게 관리	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
12.3	네트워크 인프라를 안전하게 관리	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.3	네트워크 인프라를 안전하게 관리	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
12.3	네트워크 인프라를 안전하게 관리	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.3	네트워크 인프라를 안전하게 관리	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
12.3	네트워크 인프라를 안전하게 관리	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
12.6	보안 네트워크 관리 및 통신 프로토콜 사용	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13.1	보안 이벤트 알림 중앙 집중화	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13.1	보안 이벤트 알림 중앙 집중화	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13.3	네트워크 침입 탐지 솔루션 배포	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
13.6	네트워크 트래픽 흐름 로그 수집	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13.6	네트워크 트래픽 흐름 로그 수집	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
13.10	애플리케이션 계층 필터링 수행	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16.1	안전한 애플리케이션 개발 프로세스 수립 및 유지	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
16.1	안전한 애플리케이션 개발 프로세스 수립 및 유지	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 보안 인증 정보가 포함되지 않도록 합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16.1	안전한 애플리케이션 개발 프로세스 수립 및 유지	codebuild-project-environment-privileged-check	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있지 않은지 확인합니다. Docker API와 컨테이너의 기본 하드웨어에 대해 의도하지 않은 액세스를 방지하려면 이 설정을 비활성화해야 합니다.
16.1	안전한 애플리케이션 개발 프로세스 수립 및 유지	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.
16.1	안전한 애플리케이션 개발 프로세스 수립 및 유지	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16.12	코드 수준 보안 검사 구현	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
16.12	코드 수준 보안 검사 구현	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 보안 인증 정보가 포함되지 않도록 합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16.12	코드 수준 보안 검사 구현	codebuild-project-environment-privileged-check	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있지 않은지 확인합니다. Docker API와 컨테이너의 기본 하드웨어에 대해 의도하지 않은 액세스를 방지하려면 이 설정을 비활성화해야 합니다.
16.12	코드 수준 보안 검사 구현	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.
16.12	코드 수준 보안 검사 구현	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

템플릿

템플릿은 GitHub: Operational Best Practices for CIS Critical Security Controls v8 IG3에서 확인할 수 있습니다.

CIS 운영 모범 사례 상위 20개

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 CIS(인터넷 보안 센터) 상위 20가지 중요 보안 제어와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 CIS 상위 20개 제어와 관련이 있습니다. CIS 제어 기능 상위 20개는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 적합성 팩은 Payment Card Industry Qualified Security Assessors(QSAs), HITRUST Certified Common Security Framework Practitioners(CCSFPs AWS) 및 다양한 산업 프레임워크에 대한 지침과 평가를 제공하도록 인증된 규정 준수 전문가로 구성된 팀인 AWS Security Assurance Services LLC(SAS)에서 검증되었습니다. AWS SAS 전문가는 고객이 CIS Top 20의 하위 집합에 맞게이 적합성 팩을 설계했습니다.

제어 ID	AWS Config 규칙	지침
CIS.2	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	AWS Config 규칙	지침
CIS.2	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
CIS.2	ec2-security-group-attached-to-eni	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.
CIS.2	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.2	ec2-volume-inuse-check	이 규칙 덕분에 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨은 인스턴스 종료 시 삭제 대상으로 표시됩니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.
CIS.2	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
CIS.3	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS Config 규칙	지침
CIS.3	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
CIS.3	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.4	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CIS.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CIS.4	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS Config 규칙	지침
CIS.4	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CIS.4	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS Config 규칙	지침
CIS.4	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
CIS.5	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	AWS Config 규칙	지침
CIS.5	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CIS.5	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	AWS Config 규칙	지침
CIS.5	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
CIS.5	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.6	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
CIS.6	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
CIS.6	cloudtrail-enabled	AWS CloudTrail 는 Management Console 작업 및 API 호출을 기록 AWS 하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.6	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
CIS.6	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	AWS Config 규칙	지침
CIS.6	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
CIS.6	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.6	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CIS.6	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.6	multi-region-cloudtrail-enabled	AWS CloudTrail 는 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든에서 S3 버킷 AWS 리전 으로 로그 파일을 전송합니다. 또한 AWS 에서 새 리전을 시작하면 CloudTrail은 새 리전에 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	AWS Config 규칙	지침
CIS.6	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
CIS.6	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS Config 규칙	지침
CIS.6	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
CIS.6	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS Config 규칙	지침
CIS.8	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CIS.9	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIS.9	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS Config 규칙	지침
CIS.9	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIS.9	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CIS.9	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS Config 규칙	지침
CIS.9	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
CIS.9	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	AWS Config 규칙	지침
CIS.9	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CIS.9	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.9	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
CIS.9	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS Config 규칙	지침
CIS.9	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIS.9	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS Config 규칙	지침
CIS.9	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.9	s3-account-level-public-access-blocks	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
CIS.9	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.9	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CIS.9	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CIS.9	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS Config 규칙	지침
CIS.9	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CIS.10	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CIS.10	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	AWS Config 규칙	지침
CIS.10	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CIS.10	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CIS.10	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	AWS Config 규칙	지침
CIS.11	ec2-security-group-attached-to-eni	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.
CIS.11	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS Config 규칙	지침
CIS.11	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
CIS.11	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS Config 규칙	지침
CIS.11	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CIS.12	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIS.12	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS Config 규칙	지침
CIS.12	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIS.12	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CIS.12	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS Config 규칙	지침
CIS.12	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CIS.12	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS Config 규칙	지침
CIS.12	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
CIS.12	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.12	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
CIS.12	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.12	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIS.12	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIS.12	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS Config 규칙	지침
CIS.12	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.12	s3-account-level-public-access-blocks	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
CIS.12	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.12	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CIS.12	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CIS.12	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.12	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
CIS.12	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.13	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
CIS.13	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.13	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
CIS.13	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS Config 규칙	지침
CIS.13	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
CIS.13	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.13	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CIS.13	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS Config 규칙	지침
CIS.13	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
CIS.13	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CIS.13	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS Config 규칙	지침
CIS.13	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
CIS.13	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.13	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS Config 규칙	지침
CIS.13	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
CIS.13	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.13	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.

제어 ID	AWS Config 규칙	지침
CIS.13	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.13	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.13	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS Config 규칙	지침
CIS.13	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.13	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.14	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.14	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.14	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
CIS.14	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
CIS.14	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS Config 규칙	지침
CIS.14	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIS.14	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIS.14	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.14	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS Config 규칙	지침
CIS.14	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CIS.14	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
CIS.14	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	AWS Config 규칙	지침
CIS.14	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.
CIS.14	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS Config 규칙	지침
CIS.14	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
CIS.14	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIS.14	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS Config 규칙	지침
CIS.14	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIS.14	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.14	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS Config 규칙	지침
CIS.14	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.14	s3-account-level-public-access-blocks	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.14	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.
CIS.14	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
CIS.14	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.14	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CIS.14	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.14	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS Config 규칙	지침
CIS.14	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.14	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIS.14	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS Config 규칙	지침
CIS.16	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
CIS.16	cloudtrail-enabled	AWS CloudTrail 는 Management Console 작업 및 API 호출을 기록 AWS 하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.16	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.16	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.
CIS.16	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS Config 규칙	지침
CIS.16	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.16	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 CIS(인터넷 보안 센터) AWS 파운데이션 벤치마크의 암호 강도에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
CIS.16	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
CIS.16	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.16	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
CIS.16	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
CIS.16	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS Config 규칙	지침
CIS.16	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CIS.16	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS Config 규칙	지침
CIS.16	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
CIS.16	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
CIS.16	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.16	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
CIS.18	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.18	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 보안 인증 정보가 포함되지 않도록 합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
CIS.19	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS Config 규칙	지침
CIS.19	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
CIS.19	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS Config 규칙	지침
CIS.2	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

템플릿

템플릿은 GitHub: CIS 운영 모범 사례 상위 20개에서 확인할 수 있습니다.

CISA Cyber Essentials의 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 사이버 보안 및 인프라 보안 기관(CISA) 사이버 필수 요소(CE)와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 AWS Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 CISA CE 제어와 관련이 있습니다. CISA CE 제어는 여러 AWS Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
직원-1	직원들이 온라인에서 올바른 선택을 하도록 독려하는 인식 문화를 조성하세요.	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지하세요. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.
직원-2	피싱 및 비즈니스 이메일 침해와 같은 위험에 대해 알아보세요.XXXXX.	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지하세요. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.
직원-3	교훈을 얻고 보고된 이벤트를 활용하여 현재의 위협 환경에 대한 경계를 유지하고 사이버 보안 동향에 민첩하게 대응함으로써 사이버 보안과 관련된 최신 이벤트를 지속적으로 인지합니다.	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지하세요. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.
직원-4	기본 사이버 보안 교육을 활용하여 사이버 보안 모범 사례 구현과 관련된 사이버 보안 개념, 용어 및 활동에 대한 노출을 개선하세요.	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지하세요. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법

제어 ID	제어 설명	AWS 구성 규칙	지침
			을 직원들에게 교육합니다.
직원-5	전문 협회, 학술 기관, 민간 부문 및 정부 출처를 통해 이용 가능한 교육 리소스를 확인하세요.	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지하세요. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.
사용자 시스템-1	네트워크에 무엇이 있는지 알아보세요. 하드웨어 및 소프트웨어 자산의 인벤토리를 관리하여 사용 중이거나 공격의 위험에 노출된 자산을 파악하세요.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-1	네트워크에 무엇이 있는지 알아보세요. 하드웨어 및 소프트웨어 자산의 인벤토리를 관리하여 사용 중이거나 공격의 위험에 노출된 자산을 파악하세요.	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
사용자 시스템-1	네트워크에 무엇이 있는지 알아보세요. 하드웨어 및 소프트웨어 자산의 인벤토리를 관리하여 사용 중이거나 공격의 위험에 노출된 자산을 파악하세요.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-1	네트워크에 무엇이 있는지 알아보세요. 하드웨어 및 소프트웨어 자산의 인벤토리를 관리하여 사용 중이거나 공격의 위험에 노출된 자산을 파악하세요.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
사용자 시스템-1	네트워크에 무엇이 있는지 알아보세요. 하드웨어 및 소프트웨어 자산의 인벤토리를 관리하여 사용 중이거나 공격의 위험에 노출된 자산을 파악하세요.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-1	네트워크에 무엇이 있는지 알아보세요. 하드웨어 및 소프트웨어 자산의 인벤토리를 관리하여 사용 중이거나 공격의 위험에 노출된 자산을 파악하세요.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
사용자 시스템-1	네트워크에 무엇이 있는지 알아보세요. 하드웨어 및 소프트웨어 자산의 인벤토리를 관리하여 사용 중이거나 공격의 위험에 노출된 자산을 파악하세요.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-2	모든 운영 체제 및 타사 소프트웨어에 대한 자동 업데이트를 활용합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
사용자 시스템-2	모든 운영 체제 및 타사 소프트웨어에 대한 자동 업데이트를 활용합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-2	모든 운영 체제 및 타사 소프트웨어에 대한 자동 업데이트를 활용합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-2	모든 운영 체제 및 타사 소프트웨어에 대한 자동 업데이트를 활용합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 RDBMS(Relational Database Management System)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service(OpenSearch Service)의 고가용성과 내결함성을 위해서는 최소한 3개 이상의 데이터 노드가 필요합니다. 3개 이상의 데이터 노드가 포함된 OpenSearch Service 도메인을 배포하면 노드에 장애가 발생하더라도 클러스터 운영이 보장됩니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	secretsmanager-secret-periodic-rotation	이 규칙은 AWS Secrets Manager 보안 암호에 주기적 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다. 기본값은 90일입니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	secretsmanager-secret-unused	AWS Secrets Manager에 미사용 자격 증명이 있는 경우 자격 증명을 비활성화 및/또는 제거해야 합니다. 최소 권한 원칙을 위반할 수 있습니다. 이 규칙을 사용하면 값을 unusedForDays(Config 기본값: 90)로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
사용자 시스템-3	모든 하드웨어 및 소프트웨어 자산에 대한 보안 구성을 구현하세요.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 시스템-4	지원되지 않거나 승인되지 않은 하드웨어 및 소프트웨어를 시스템에서 제거합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
주변 환경-1	네트워크에 누가 있는지 알아보세요. 네트워크 연결(사용자, 공급업체, 비즈니스 파트너 등)의 인벤토리를 관리하세요.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
주변 환경-1	네트워크에 누가 있는지 알아보세요. 네트워크 연결(사용자, 공급업체, 비즈니스 파트너 등)의 인벤토리를 관리하세요.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
주변 환경-1	네트워크에 누가 있는지 알아보세요. 네트워크 연결(사용자, 공급업체, 비즈니스 파트너 등)의 인벤토리를 관리하세요.	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
주변 환경-2	권한이 있는 사용자, 관리 사용자, 원격 액세스 사용자를 비롯한 모든 사용자에 대해 다중 인증(MFA)을 활용하세요.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
주변 환경-2	권한이 있는 사용자, 관리 사용자, 원격 액세스 사용자를 비롯한 모든 사용자에 대해 다중 인증(MFA)을 활용하세요.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
주변 환경-2	권한이 있는 사용자, 관리 사용자, 원격 액세스 사용자를 비롯한 모든 사용자에 대해 다중 인증(MFA)을 활용하세요.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
주변 환경-2	권한이 있는 사용자, 관리 사용자, 원격 액세스 사용자를 비롯한 모든 사용자에 대해 다중 인증(MFA)을 활용하세요.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
주변 환경-3	알아야 할 사항 및 최소 권한에 따라 액세스 및 관리자 권한을 부여하세요.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
주변 환경-3	알아야 할 사항 및 최소 권한에 따라 액세스 및 관리자 권한을 부여하세요.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
주변 환경-3	알아야 할 사항 및 최소 권한에 따라 액세스 및 관리자 권한을 부여하세요.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
주변 환경-3	알아야 할 사항 및 최소 권한에 따라 액세스 및 관리자 권한을 부여하세요.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
주변 환경-3	알아야 할 사항 및 최소 권한에 따라 액세스 및 관리자 권한을 부여하세요.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
주변 환경-3	알아야 할 사항 및 최소 권한에 따라 액세스 및 관리자 권한을 부여하세요.	secretsmanager-secret-unused	AWS Secrets Manager에 미사용 자격 증명이 있는 경우 자격 증명을 비활성화 및/또는 제거해야 합니다. 최소 권한 원칙을 위반할 수 있습니다. 이 규칙을 사용하면 값을 unusedForDays(Config 기본값: 90)로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
주변 환경-3	알아야 할 사항 및 최소 권한에 따라 액세스 및 관리자 권한을 부여하세요.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
주변 환경-3	모든 사용자의 고유한 비밀번호를 활용하세요.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-1	데이터가 어떻게 보호되는지 알아보세요.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-2	네트워크에서 발생하는 상황을 파악하고 네트워크 및 경계 구성 요소, 호스트 및 장치 구성 요소, 저장 데이터 및 전송 중인 데이터, 사용자 행동 활동을 관리합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
사용자 데이터-3	도메인 네임 시스템 보호.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
사용자 데이터-4	정기적인 자동 백업 및 주요 시스템 중복을 설정합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
사용자 데이터-5	물리적 보안, 암호화 및 오프라인 사본을 포함한 백업 보호 기능을 활용하세요.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
사용자 데이터-5	물리적 보안, 암호화 및 오프라인 사본을 포함한 백업 보호 기능을 활용하세요.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
위기 대응-2	공격을 탐지, 전달 및 억제하기 위한 내부 보고 구조 개발을 주도하세요.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
위기 대응-2	공격을 탐지, 전달 및 억제하기 위한 내부 보고 구조 개발을 주도하세요.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 사용하세요.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-1	중요한 데이터 및 시스템 구성을 자동으로 계속 백업하는 백업 솔루션을 활용하세요.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
부팅: 먼저 해야 할 일-2	가능하다면 시스템에 액세스할 때 다중 인증(MFA)이 필요합니다. MFA는 모든 사용자에게 필수이지만 권한이 있는 관리자 및 원격 액세스 사용자부터 시작해야 합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-2	가능하다면 시스템에 액세스할 때 다중 인증(MFA)이 필요합니다. MFA는 모든 사용자에게 필수이지만 권한이 있는 관리자 및 원격 액세스 사용자부터 시작해야 합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-2	가능하다면 시스템에 액세스할 때 다중 인증(MFA)이 필요합니다. MFA는 모든 사용자에게 필수이지만 권한이 있는 관리자 및 원격 액세스 사용자부터 시작해야 합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
부팅: 먼저 해야 할 일-2	가능하다면 시스템에 액세스할 때 다중 인증(MFA)이 필요합니다. MFA는 모든 사용자에게 필수이지만 권한이 있는 관리자 및 원격 액세스 사용자부터 시작해야 합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-3	가능하다면 자동 업데이트를 활성화하세요. 지원되지 않는 운영 체제, 애플리케이션 및 하드웨어를 교체합니다. 패치를 빠르게 테스트하고 배포하세요.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
부팅: 먼저 해야 할 일-3	가능하다면 자동 업데이트를 활성화하세요. 지원되지 않는 운영 체제, 애플리케이션 및 하드웨어를 교체합니다. 패치를 빠르게 테스트하고 배포하세요.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 RDBMS(Relational Database Management System)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-3	가능하다면 자동 업데이트를 활성화하세요. 지원되지 않는 운영 체제, 애플리케이션 및 하드웨어를 교체합니다. 패치를 빠르게 테스트하고 배포하세요.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
부팅: 먼저 해야 할 일-3	가능하다면 자동 업데이트를 활성화하세요. 지원되지 않는 운영 체제, 애플리케이션 및 하드웨어를 교체합니다. 패치를 빠르게 테스트하고 배포하세요.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

템플릿

템플릿은 GitHub: CISA Cyber Essentials 운영 모범 사례에서 확인할 수 있습니다.

미국 연방수사국 형사사법정보부(CJIS) 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 CJIS(Criminal Justice Information Services) 규정 준수 요구 사항과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 CJIS 제어와 관련이 있습니다. CJIS 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.2	보안 인식 교육	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.
5.3	인시던트 대응	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되는지 확인하세요. 대응 계획을 업데이트하고 공식적으로 문서화하면 대응 담당자가 역할, 책임 및 사고 발생 시 따라야 할 프로세스를 이해하는 데 도움이 될 수 있습니다.
5.3	인시던트 대응	response-plan-tested(프로세스 확인)	사고 대응 및 복구 계획이 테스트되었는지 확인합니다. 이는 인시던트 발생 중에 해당 계획이 효과적인지 그리고 격차나 업데이트를 해결해야 하는지를 이해하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4	감사 및 책임	audit-log-policy-exists(프로세스 확인)	조직의 로깅 요구 사항을 정의하는 감사 로그 관리 정책을 수립하고 유지 관리합니다. 여기에는 감사 로그의 검토 및 보존이 포함되며 이에 국한되지는 않습니다.
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	codebuild-project-s3-logs-encrypted	저장 시 민감한 데이터를 보호하려면 Amazon S3에 저장된 your AWS CodeBuild 로그에 암호화가 활성화되어 있는지 확인하세요.
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하기 때문에 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
5.4.1	감사 가능한 이벤트 및 콘텐츠(정보 시스템)	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4.5	감사 정보 보호	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
5.4.5	감사 정보 보호	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.4.5	감사 정보 보호	codebuild-project-s3-logs-encrypted	저장 시 민감한 데이터를 보호하려면 Amazon S3에 저장된 your AWS CodeBuild 로그에 암호화가 활성화되어 있는지 확인하세요.
5.4.6	감사 기록 보존	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하기 때문에 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
5.4.6	감사 기록 보존	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2	액세스 적용	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
5.5.2	액세스 적용	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2	액세스 적용	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2	액세스 적용	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2	액세스 적용	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 IAM 암호 정책에 대해 RequireUppercaseCharacters(CJIS 값: false), RequireLowercaseCharacters(CJIS 값: false), RequireSymbols(CJIS 값: false), RequireNumbers(CJIS 값: false), MinimumPasswordLength(CJIS 값: 8), PasswordReusePrevention(CJIS 값: 10), MaxPasswordAge(CJIS 값: 90) 등을 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2	액세스 적용	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
5.5.2	액세스 적용	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2	액세스 적용	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
5.5.2	액세스 적용	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2	액세스 적용	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
5.5.2	액세스 적용	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2	액세스 적용	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2	액세스 적용	rds-instance-iam-authentication-enabled	시스템 및 자산에 대한 액세스를 제어하기 위해 Amazon Relational Database Service(Amazon RDS) 인스턴스에서 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. 이렇게 하면 데이터베이스를 오가는 네트워크 트래픽이 SSL(Secure Sockets Layer)을 통해 암호화됩니다. 인증은 외부에서 관리되므로 사용자 보안 인증 정보를 데이터베이스에 저장할 필요가 없습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2	액세스 적용	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.
5.5.2.1	최소 권한	codebuild-project-environment-privileged-check	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있지 않은지 확인하세요. Docker API와 컨테이너의 기본 하드웨어에 대해 의도하지 않은 액세스를 방지하려면 이 설정을 비활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2.1	최소 권한	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2.1	최소 권한	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2.1	최소 권한	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2.1	최소 권한	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
5.5.2.1	최소 권한	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2.1	최소 권한	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
5.5.2.1	최소 권한	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2.1	최소 권한	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2.1	최소 권한	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).
5.5.2.1	최소 권한	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2.1	최소 권한	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.
5.5.2.1	최소 권한	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.2.1	최소 권한	secretsmanager-secret-unused	AWS Secrets Manager에 미사용 자격 증명이 있는 경우 자격 증명을 비활성화 및/또는 제거해야 합니다. 최소 권한 원칙을 위반할 수 있습니다. 이 규칙을 사용하면 값을 unusedForDays(Config 기본값: 90)로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.6	원격 액세스	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.5.6	원격 액세스	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.6.2.1.1	암호	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 IAM 암호 정책에 대해 RequireUppercaseCharacters(CJIS 값: false), RequireLowercaseCharacters(CJIS 값: false), RequireSymbols(CJIS 값: false), RequireNumbers(CJIS 값: false), MinimumPasswordLength(CJIS 값: 8), PasswordReusePrevention(CJIS 값: 10), MaxPasswordAge(CJIS 값: 90) 등을 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.6.2.2	고급 인증	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.6.2.2	고급 인증	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
5.6.2.2	고급 인증	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.6.2.2	고급 인증	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
5.6.2.2	고급 인증	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.6.3.1	식별자 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
5.7.1.1	최소 자릿수	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
5.7.1.1	최소 자릿수	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
5.7.1.1	최소 자릿수	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
5.7.1.1	최소 자릿수	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
5.7.1.1	최소 자릿수	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
5.7.1.1	최소 자릿수	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
5.7.1.1	최소 자릿수	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
5.7.1.1	최소 자릿수	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.7.1.1	최소 자릿수	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
5.7.1.1	최소 자릿수	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10	시스템 및 통신 보호와 정보 무결성	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10	시스템 및 통신 보호와 정보 무결성	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10	시스템 및 통신 보호와 정보 무결성	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
5.10	시스템 및 통신 보호와 정보 무결성	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10	시스템 및 통신 보호와 정보 무결성	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10	시스템 및 통신 보호와 정보 무결성	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10	시스템 및 통신 보호와 정보 무결성	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10	시스템 및 통신 보호와 정보 무결성	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10	시스템 및 통신 보호와 정보 무결성	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10	시스템 및 통신 보호와 정보 무결성	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10	시스템 및 통신 보호와 정보 무결성	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10	시스템 및 통신 보호와 정보 무결성	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
5.10	시스템 및 통신 보호와 정보 무결성	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.
5.10.1	정보 흐름 적용	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1	정보 흐름 적용	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1	정보 흐름 적용	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
5.10.1	정보 흐름 적용	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
5.10.1	정보 흐름 적용	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
5.10.1	정보 흐름 적용	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
5.10.1	정보 흐름 적용	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1	정보 흐름 적용	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
5.10.1	정보 흐름 적용	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
5.10.1	정보 흐름 적용	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
5.10.1	정보 흐름 적용	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1	정보 흐름 적용	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
5.10.1.1	경계 보호	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.1	경계 보호	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
5.10.1.1	경계 보호	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.1	경계 보호	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.1	경계 보호	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.1	경계 보호	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.1	경계 보호	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
5.10.1.1	경계 보호	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
5.10.1.1	경계 보호	waf-regional-rule-not-empty	AWS WAF에 비어 있지 않은 규칙이 있는지 확인합니다. 조건이 없는 규칙에는 의도하지 않은 동작이 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.1	경계 보호	waf-regional-rulegroup-not-empty	AWS WAF에 비어 있지 않은 규칙 그룹이 있는지 확인합니다. 규칙 그룹이 비어 있으면 의도하지 않은 동작이 발생할 수 있습니다.
5.10.1.1	경계 보호	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.
5.10.1.2	암호화	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.2	암호화	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
5.10.1.2	암호화	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail의 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
5.10.1.2	암호화	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
5.10.1.2	암호화	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.
5.10.1.2	암호화	codebuild-project-s3-logs-encrypted	저장 시 민감한 데이터를 보호하려면 Amazon S3에 저장된 your AWS CodeBuild 로그에 대해 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
5.10.1.2	암호화	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.2	암호화	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
5.10.1.2	암호화	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
5.10.1.2	암호화	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.2	암호화	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
5.10.1.2	암호화	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Kinesis Streams에 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.2	암호화	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
5.10.1.2	암호화	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.2	암호화	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.2	암호화	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.2	암호화	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.2	암호화	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.2	암호화	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.2	암호화	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.2	암호화	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5.10.1.3	침입 탐지 도구 및 기법	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.3	침입 탐지 도구 및 기법	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.1.3	침입 탐지 도구 및 기법	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.4.1	패치 관리	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.4.1	패치 관리	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
5.10.4.1	패치 관리	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.4.1	패치 관리	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. AWS Fargate 플랫폼 버전에 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.
5.10.4.1	패치 관리	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.4.4	보안 알림 및 권고 사항	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
5.10.4.4	보안 알림 및 권고 사항	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.10.4.4	보안 알림 및 권고 사항	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

템플릿

템플릿은 GitHub: CJIS 운영 모범 사례에서 확인할 수 있습니다.

CMMC 2.0 레벨 1 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 사이버 보안 성숙도 모델 인증(CMMC) 2.0 레벨 1과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 CMMC 2.0 레벨 1 제어와 관련이 있습니다. CMMC 2.0 레벨 1 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한

제어 ID	제어 설명	AWS 구성 규칙	지침
			계정에는 액세스 제어가 필요합니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	rds-instance-public-access-check	Amazon Relational Database Service(A mazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	rds-instance-public-access-check	Amazon Relational Database Service(A mazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 마스터 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L1-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
IA.L1-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L1-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
IA.L1-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L1-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L1-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L1-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L1-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
IA.L1-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L1-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L1-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L1-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IA.L1-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L1-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L1-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA.L1-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L1-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L1-3.14.1	정보 및 정보 시스템 결함을 적시에 식별, 보고 및 수정합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L1-3.14.1	정보 및 정보 시스템 결함을 적시에 식별, 보고 및 수정합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L1-3.14.1	정보 및 정보 시스템 결함을 적시에 식별, 보고 및 수정합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L1-3.14.2	조직 정보 시스템 내의 적절한 위치에서 악성 코드로부터 보호합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SI.L1-3.14.5	파일을 다운로드하거나 열거나 실행할 때 정보 시스템을 정기적으로 검사하고 외부 소스에서 파일을 실시간으로 검색합니다.	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository(ECR) 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.

템플릿

템플릿은 GitHub: CMMC 2.0 레벨 1 운영 모범 사례에서 확인할 수 있습니다.

CMMC 2.0 레벨 2 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제

공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 사이버 보안 성숙도 모델 인증(CMMC) 2.0 레벨 2와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 CMMC 2.0 레벨 2 제어와 관련이 있습니다. CMMC 2.0 레벨 2 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	스템 포함)로 제한합니다.		DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	rds-instance-public-access-check	Amazon Relational Database Service(A mazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.1	정보 시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 또는 디바이스(기타 정보 시스템 포함)로 제한합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	rds-instance-public-access-check	Amazon Relational Database Service(A mazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.2	정보 시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.20	외부 정보 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.4	개인들의 공모 없이 악의적인 행위의 위험을 줄이려면 업무를 분리하세요.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.4	개인들의 공모 없이 악의적인 행위의 위험을 줄이려면 업무를 분리하세요.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.4	개인들의 공모 없이 악의적인 행위의 위험을 줄이려면 업무를 분리하세요.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
AC.L2-3.1.4	개인들의 공모 없이 악의적인 행위의 위험을 줄이려면 업무를 분리하세요.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.4	개인들의 공모 없이 악의적인 행위의 위험을 줄이려면 업무를 분리하세요.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L2-3.1.4	개인들의 공모 없이 악의적인 행위의 위험을 줄이려면 업무를 분리하세요.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.4	개인들의 공모 없이 악의적인 행위의 위험을 줄이려면 업무를 분리하세요.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
AC.L2-3.1.4	개인들의 공모 없이 악의적인 행위의 위험을 줄이려면 업무를 분리하세요.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.4	개인들의 공모 없이 악의적인 행위의 위험을 줄이려면 업무를 분리하세요.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC.L2-3.1.4	개인들의 공모 없이 악의적인 행위의 위험을 줄이려면 업무를 분리하세요.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
AC.L2-3.1.5	특정 보안 기능 및 권한 있는 계정 등에는 최소 권한의 원칙을 따르세요.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.6	비보안 기능에 액세스할 때는 권한이 없는 계정이나 역할을 사용합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.6	비보안 기능에 액세스할 때는 권한이 없는 계정이나 역할을 사용합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.6	비보안 기능에 액세스할 때는 권한이 없는 계정이나 역할을 사용합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.6	비보안 기능에 액세스할 때는 권한이 없는 계정이나 역할을 사용합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.6	비보안 기능에 액세스할 때는 권한이 없는 계정이나 역할을 사용합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC.L2-3.1.6	비보안 기능에 액세스할 때는 권한이 없는 계정이나 역할을 사용합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.6	비보안 기능에 액세스할 때는 권한이 없는 계정이나 역할을 사용합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L2-3.1.6	비보안 기능에 액세스할 때는 권한이 없는 계정이나 역할을 사용합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.6	비보안 기능에 액세스할 때는 권한이 없는 계정이나 역할을 사용합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L2-3.1.6	비보안 기능에 액세스할 때는 권한이 없는 계정이나 역할을 사용합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.7	권한 없는 사용자가 권한 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사 로그에 캡처합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
AC.L2-3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
AC.L2-3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC.L2-3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC.L2-3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
AC.L2-3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC.L2-3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC.L2-3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC.L2-3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.1	불법적이거나 승인되지 않은 시스템 활동을 모니터링, 분석, 조사, 보고하는 데 필요한 범위까지 시스템 감사 로그와 기록을 생성하고 보관합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU.L2-3.3.1	불법적이거나 승인되지 않은 시스템 활동을 모니터링, 분석, 조사, 보고하는 데 필요한 범위까지 시스템 감사 로그와 기록을 생성하고 보관합니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AU.L2-3.3.1	불법적이거나 승인되지 않은 시스템 활동을 모니터링, 분석, 조사, 보고하는 데 필요한 범위까지 시스템 감사 로그와 기록을 생성하고 보관합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.1	불법적이거나 승인되지 않은 시스템 활동을 모니터링, 분석, 조사, 보고하는 데 필요한 범위까지 시스템 감사 로그와 기록을 생성하고 보관합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU.L2-3.3.1	불법적이거나 승인되지 않은 시스템 활동을 모니터링, 분석, 조사, 보고하는 데 필요한 범위까지 시스템 감사 로그와 기록을 생성하고 보관합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.1	불법적이거나 승인되지 않은 시스템 활동을 모니터링, 분석, 조사, 보고하는 데 필요한 범위까지 시스템 감사 로그와 기록을 생성하고 보관합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.1	불법적이거나 승인되지 않은 시스템 활동을 모니터링, 분석, 조사, 보고하는 데 필요한 범위까지 시스템 감사 로그와 기록을 생성하고 보관합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.1	불법적이거나 승인되지 않은 시스템 활동을 모니터링, 분석, 조사, 보고하는 데 필요한 범위까지 시스템 감사 로그와 기록을 생성하고 보관합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AU.L2-3.3.1	불법적이거나 승인되지 않은 시스템 활동을 모니터링, 분석, 조사, 보고하는 데 필요한 범위까지 시스템 감사 로그와 기록을 생성하고 보관합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.1	불법적이거나 승인되지 않은 시스템 활동을 모니터링, 분석, 조사, 보고하는 데 필요한 범위까지 시스템 감사 로그와 기록을 생성하고 보관합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
AU.L2-3.3.2	개별 시스템 사용자의 행동을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 행동에 대해 책임을 질 수 있도록 하세요.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.2	개별 시스템 사용자의 행동을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 행동에 대해 책임을 질 수 있도록 하세요.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AU.L2-3.3.2	개별 시스템 사용자의 행동을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 행동에 대해 책임을 질 수 있도록 하세요.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.2	개별 시스템 사용자의 행동을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 행동에 대해 책임을 질 수 있도록 하세요.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU.L2-3.3.2	개별 시스템 사용자의 행동을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 행동에 대해 책임을 질 수 있도록 하세요.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.2	개별 시스템 사용자의 행동을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 행동에 대해 책임을 질 수 있도록 하세요.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.2	개별 시스템 사용자의 행동을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 행동에 대해 책임을 질 수 있도록 하세요.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AU.L2-3.3.2	개별 시스템 사용자의 행동을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 행동에 대해 책임을 질 수 있도록 하세요.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.2	개별 시스템 사용자의 행동을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 행동에 대해 책임을 질 수 있도록 하세요.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.4	감사 로깅 프로세스 실패 시 알립니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
AU.L2-3.3.4	감사 로깅 프로세스 실패 시 알립니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.4	감사 로깅 프로세스 실패 시 알립니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.4	감사 로깅 프로세스 실패 시 알립니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.5	감사 기록 검토, 분석 및 보고 프로세스를 상호 연계하여 불법적이거나 승인되지 않았거나 의심스럽거나 특이한 활동의 징후에 대한 조사 및 대응을 수행합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.5	감사 기록 검토, 분석 및 보고 프로세스를 상호 연계하여 불법적이거나 승인되지 않았거나 의심스럽거나 특이한 활동의 징후에 대한 조사 및 대응을 수행합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU.L2-3.3.8	감사 정보 및 감사 로깅 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CA.L2-3.12.2	조직 시스템의 결함을 수정하고 취약성을 줄이거나 없애기 위해 설계된 실행 계획을 개발하고 구현합니다.	vuln-management-plan-exists(프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 프로세스를 공식적으로 정의하려면 취약성 관리 계획을 개발하고 구현해야 합니다. 여기에는 취약성 관리 도구, 환경 검사 주기, 역할 및 책임이 포함될 수 있습니다.
CA.L2-3.12.3	보안 통제를 지속적으로 모니터링하여 통제의 효과가 지속되도록 하세요.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA.L2-3.12.3	보안 통제를 지속적으로 모니터링하여 통제의 효과가 지속되도록 하세요.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA.L2-3.12.3	보안 통제를 지속적으로 모니터링하여 통제의 효과가 지속되도록 하세요.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.1	각 시스템 개발 주기 전반에 걸쳐 조직 시스템(하드웨어, 소프트웨어, 펌웨어, 문서 포함)의 기본 구성 및 인벤토리를 수립하고 유지합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
CM.L2-3.4.1	각 시스템 개발 주기 전반에 걸쳐 조직 시스템(하드웨어, 소프트웨어, 펌웨어, 문서 포함)의 기본 구성 및 인벤토리를 수립하고 유지합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.1	각 시스템 개발 주기 전반에 걸쳐 조직 시스템(하드웨어, 소프트웨어, 펌웨어, 문서 포함)의 기본 구성 및 인벤토리를 수립하고 유지합니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
CM.L2-3.4.1	각 시스템 개발 주기 전반에 걸쳐 조직 시스템(하드웨어, 소프트웨어, 펌웨어, 문서 포함)의 기본 구성 및 인벤토리를 수립하고 유지합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.1	각 시스템 개발 주기 전반에 걸쳐 조직 시스템(하드웨어, 소프트웨어, 펌웨어, 문서 포함)의 기본 구성 및 인벤토리를 수립하고 유지합니다.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
CM.L2-3.4.2	조직 시스템에 사용되는 정보 기술 제품에 대한 보안 구성 설정을 수립하고 적용합니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.2	조직 시스템에 사용되는 정보 기술 제품에 대한 보안 구성 설정을 수립하고 적용합니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
CM.L2-3.4.2	조직 시스템에 사용되는 정보 기술 제품에 대한 보안 구성 설정을 수립하고 적용합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.2	조직 시스템에 사용되는 정보 기술 제품에 대한 보안 구성 설정을 수립하고 적용합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.2	조직 시스템에 사용되는 정보 기술 제품에 대한 보안 구성 설정을 수립하고 적용합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
CM.L2-3.4.2	조직 시스템에 사용되는 정보 기술 제품에 대한 보안 구성 설정을 수립하고 적용합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.2	조직 시스템에 사용되는 정보 기술 제품에 대한 보안 구성 설정을 수립하고 적용합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
CM.L2-3.4.2	조직 시스템에 사용되는 정보 기술 제품에 대한 보안 구성 설정을 수립하고 적용합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.2	조직 시스템에 사용되는 정보 기술 제품에 대한 보안 구성 설정을 수립하고 적용합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.2	조직 시스템에 사용되는 정보 기술 제품에 대한 보안 구성 설정을 수립하고 적용합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.2	조직 시스템에 사용되는 정보 기술 제품에 대한 보안 구성 설정을 수립하고 적용합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.3	조직 시스템의 변경 사항을 추적, 검토, 승인 또는 거부하고 기록합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용하세요.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.7	불필요한 프로그램, 기능, 포트, 프로토콜 및 서비스의 사용을 제한, 비활성화 또는 금지합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.9	사용자가 설치한 소프트웨어를 제어 및 모니터링합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM.L2-3.4.9	사용자가 설치한 소프트웨어를 제어 및 모니터링합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
CM.L2-3.4.9	사용자가 설치한 소프트웨어를 제어 및 모니터링합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
IA.L2-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
IA.L2-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
IA.L2-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.1	사용자 또는 디바이스를 대신하여 활동하는 정보 시스템 사용자, 프로세스를 식별합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IA.L2-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA.L2-3.5.2	조직 정보 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 디바이스의 ID를 인증(또는 확인)합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.3	권한 있는 계정에 대한 로컬 및 네트워크 액세스와 권한 없는 계정에 대한 네트워크 액세스에 대해서는 다중 인증을 사용합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
IA.L2-3.5.3	권한 있는 계정에 대한 로컬 및 네트워크 액세스와 권한 없는 계정에 대한 네트워크 액세스에 대해서는 다중 인증을 사용합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.3	권한 있는 계정에 대한 로컬 및 네트워크 액세스와 권한 없는 계정에 대한 네트워크 액세스에 대해서는 다중 인증을 사용합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA.L2-3.5.3	권한 있는 계정에 대한 로컬 및 네트워크 액세스와 권한 없는 계정에 대한 네트워크 액세스에 대해서는 다중 인증을 사용합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.6	지정된 기간 동안 활동이 없으면 식별자를 비활성화합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IA.L2-3.5.6	지정된 기간 동안 활동이 없으면 식별자를 비활성화합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.7	새 암호를 만들 때 암호 복잡성과 문자 변경을 최소화합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.8	지정된 세대 수에 대한 암호 재사용을 금지합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장되어 있을 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
IA.L2-3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR.L2-3.6.1	준비, 탐지, 분석, 격리, 복구 및 사용자 대응 활동을 포함하는 조직 시스템의 운영 인시던트 처리 역량을 구축합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
IR.L2-3.6.1	준비, 탐지, 분석, 격리, 복구 및 사용자 대응 활동을 포함하는 조직 시스템의 운영 인시던트 처리 역량을 구축합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR.L2-3.6.1	준비, 탐지, 분석, 격리, 복구 및 사용자 대응 활동을 포함하는 조직 시스템의 운영 인시던트 처리 역량을 구축합니다.	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.
IR.L2-3.6.1	준비, 탐지, 분석, 격리, 복구 및 사용자 대응 활동을 포함하는 조직 시스템의 운영 인시던트 처리 역량을 구축합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR.L2-3.6.3	조직의 사고 대응 능력을 테스트하세요.	response-plan-tested(프로세스 확인)	사고 대응 및 복구 계획이 테스트되었는지 확인합니다. 이는 인시던트 발생 중에 해당 계획이 효과적인지 그리고 격차나 업데이트를 해결해야 하는지를 이해하는 데 도움이 될 수 있습니다.
MA.L2-3.7.5	외부 네트워크 연결에서 비로컬 유지 관리 세션을 설정하고 비로컬 유지 관리가 완료될 때 이러한 연결을 종료하려면 다중 인증이 필요합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
MA.L2-3.7.5	외부 네트워크 연결에서 비로컬 유지 관리 세션을 설정하고 비로컬 유지 관리가 완료될 때 이러한 연결을 종료하려면 다중 인증이 필요합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
RA.L2-3.11.2	조직 시스템 및 애플리케이션의 취약성을 정기적으로 검사하고 해당 시스템 및 애플리케이션에 영향을 미치는 새로운 취약성이 확인되면 검사합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA.L2-3.11.2	조직 시스템 및 애플리케이션의 취약성을 정기적으로 검사하고 해당 시스템 및 애플리케이션에 영향을 미치는 새로운 취약성이 확인되면 검사합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
RA.L2-3.11.2	조직 시스템 및 애플리케이션의 취약성을 정기적으로 검사하고 해당 시스템 및 애플리케이션에 영향을 미치는 새로운 취약성이 확인되면 검사합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA.L2-3.11.2	조직 시스템 및 애플리케이션의 취약성을 정기적으로 검사하고 해당 시스템 및 애플리케이션에 영향을 미치는 새로운 취약성이 확인되면 검사합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.1	정보 시스템의 외부 경계 및 주요 내부 경계에서 조직 통신(즉, 조직 정보 시스템이 전송했거나 수신한 정보)을 모니터링, 제어 및 보호합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.4	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
SC.L2-3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC.L2-3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.10	조직 시스템에 사용되는 암호화를 위한 암호화 키를 설정하고 관리합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.10	조직 시스템에 사용되는 암호화를 위한 암호화 키를 설정하고 관리합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
SC.L2-3.13.15	통신 세션의 신뢰성을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.15	통신 세션의 신뢰성을 보호합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
SC.L2-3.13.15	통신 세션의 신뢰성을 보호합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.15	통신 세션의 신뢰성을 보호합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC.L2-3.13.15	통신 세션의 신뢰성을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.15	통신 세션의 신뢰성을 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장되어 있을 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC.L2-3.13.16	저장 중 CUI의 기밀을 보호합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
SI.L2-3.14.1	정보 및 정보 시스템 결함을 적시에 식별, 보고 및 수정합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.1	정보 및 정보 시스템 결함을 적시에 식별, 보고 및 수정합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.1	정보 및 정보 시스템 결함을 적시에 식별, 보고 및 수정합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.2	조직 정보 시스템 내의 적절한 위치에서 악성 코드로부터 보호합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SI.L2-3.14.5	파일을 다운로드하거나 열거나 실행할 때 정보 시스템을 정기적으로 검사하고 외부 소스에서 파일을 실시간으로 검색합니다.	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository(ECR) 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
SI.L2-3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI.L2-3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
SI.L2-3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
SI.L2-3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
SI.L2-3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI.L2-3.14.7	조직 시스템의 무단 사용을 식별합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

템플릿

템플릿은 GitHub: CMMC 2.0 레벨 2 운영 모범 사례에서 확인할 수 있습니다.

컴퓨팅 서비스 운영 모범 사례

이 적합성 팩에는 컴퓨팅 서비스에 기반한 AWS Config 규칙이 포함되어 있습니다. 자세한 내용은 Compute for any workload를 참조하세요. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 컴퓨팅 서비스 운영 모범 사례에서 확인할 수 있습니다.

데이터 복원력 운영 모범 사례

에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 데이터 복원력 운영 모범 사례에서 확인할 수 있습니다.

데이터베이스 서비스 운영 모범 사례

이 적합성 팩에는 Databases Services를 기반으로 하는 AWS Config 규칙이 포함되어 있습니다. 자세한 내용은 의 데이터베이스를 참조하세요 AWS. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 데이터베이스 서비스 운영 모범 사례에서 확인할 수 있습니다.

데이터 레이크 및 분석 서비스 운영 모범 사례

이 적합성 팩에는 Data Lakes and Analytics Services에 대한 AWS Config 규칙이 포함되어 있습니다. 자세한 내용은의 Data Lakes and Analytics를 AWS 참조하세요. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 데이터 레이크 및 분석 서비스 운영 모범 사례에서 확인할 수 있습니다.

DevOps 운영 모범 사례

이 적합성 팩에는 DevOps를 기반으로 하는 AWS Config 규칙이 포함되어 있습니다 AWS. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: DevOps 운영 모범 사례에서 확인할 수 있습니다.

EC2 운영 모범 사례

이 적합성 팩에는 EC2 기반 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: EC2 운영 모범 사례에서 확인할 수 있습니다.

암호화 및 키 관리 운영 모범 사례

에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 암호화 및 키 관리 운영 모범 사례에서 확인할 수 있습니다.

SME를 위한 ENISA 사이버 보안 가이드 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 SMEs와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 SMEs. SME 제어를 위한 ENISA 사이버 보안 가이드는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 샘플 적합성 팩 템플릿에는 SME를 위한 ENISA 사이버 보안 가이드에서 채택한 제어에 대한 매핑이 포함되어 있습니다. SME를 위한 ENISA 사이버 보안 가이드는 Cybersecurity guide for SMEs - 12 steps to securing your business에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 사이버 보안 정책 게시	사이버 보안에서는 명확하고 구체적인 규칙을 제시해야 합니다.	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지하세요. 보안 인식 프로그램은 직원들에게 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 교육합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없어

제어 ID	제어 설명	AWS 구성 규칙	지침
	여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.		야 합니다. 이렇게 하면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것이 가장 좋습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elasticsearch Service(Amazon ES) 도메인에 암호화가 활성화되어 있는지 확인합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	codebuild-project-s3-logs-encrypted	저장 시 민감한 데이터를 보호하려면 Amazon S3에 저장된 your AWS CodeBuild 로그에 대해 암호화가 활성화되어 있는지 확인하세요.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	elasticsearch-node-to-node-encryption-check	Amazon Elasticsearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Kinesis Streams에 암호화를 활성화해야 합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1_좋은 사이버 보안 문화 개발: 데이터 보호 기억	EU 일반 데이터 보호 규정1에 따라 EU/EEA 거주자의 개인 데이터를 처리하거나 저장하는 모든 SME는 해당 데이터를 보호하기 위한 적절한 보안 통제책을 마련해야 합니다. 여기에는 SME를 대신하는 제3자가 적절한 보안 조치를 취하도록 하는 것이 포함됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2_적절한 교육 제공	모든 직원이 다양한 사이버 보안 위협을 인식하고 대처할 수 있도록 정기적인 사이버 보안 인식 교육을 제공합니다. 이러한 교육은 SME에 맞게 조정되어야 하며 실제 상황에 초점을 맞춰야 합니다. 비즈니스 내 사이버 보안 관리 책임자에게 전문 사이버 보안 교육을 제공하여 업무 수행에 필요한 기술과 역량을 갖추도록 하세요.	security-awareness-program-exists(Process Check)	조직을 위한 보안 인식 프로그램을 수립하고 유지하세요. 보안 인식 프로그램은 직원들에게 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 교육합니다.
4_인시던트 대응 계획 개발	모든 보안 인시던트가 적시에 전문적이고 적절한 방식으로 대응이 이루어질 수 있도록 문서화된 명확한 지침, 역할 및 책임이 포함된 공식 인시던트 대응 계획을 개발합니다. 보안 위협에 신속하게 대응하려면 의심스러운 활동이나 보안 침해가 발생할 경우 모니터링하고 경고를 생성할 수 있는 도구를 조사합니다.	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5_시스템에 대한 보안 액세스	모든 사람에게 암호 사용을 권장하세요. 이때 암호는 셋 이상의 자주 쓰이는 무작위 단어를 하나의 문구로 합쳐 기억하기 쉬우면서 안전한, 아주 좋은 조합입니다. 일반적인 암호를 선택하는 경우: - 대소문자에 숫자 및 특수문자를 포함하여 길게 만드세요. - “password”처럼 명백한 단어나 “abc”, “123 같은 문자나 숫자 순서는 피합니다. - 온라인에서 찾을 수 있는 개인 정보는 사용하지 마세요. 패스프레이즈를 사용하든 암호를 사용하든, 다른 곳에서 재사용하지 마세요. - 동료와 공유하지 마세요. - 다중 인증을 활성화합니다. - 전용 암호 관리자를 사용합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
5_시스템에 대한 보안 액세스	모든 사람에게 암호 사용을 권장하세요. 이때 암호는 셋 이상의 자주 쓰이는 무작위 단어를 하나의 문구로 합쳐 기억하기 쉬우면서 안전한, 아주 좋은 조합입니다. 일반적인 암호를 선택하는 경우: - 대소문자에 숫자 및 특수문자를 포함하여 길게 만드세요. - “password”처럼 명백한 단어나 “abc”, “123 같은 문자나 숫자 순서는 피합니다. - 온라인에서 찾을 수 있는 개인 정보는 사용하지 마세요. 패스프레이즈를 사용하든 암호를 사용하든, 다른 곳에서 재사용하지 마세요. - 동료와 공유하지 마세요. - 다중 인증을 활성화합니다. - 전용 암호 관리자를 사용합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
5_시스템에 대한 보안 액세스	모든 사람에게 암호 사용을 권장하세요. 이때 암호는 셋 이상의 자주 쓰이는 무작위 단어를 하나의 문구로 합쳐 기억하기 쉬우면서 안전한, 아주 좋은 조합입니다. 일반적인 암호를 선택하는 경우: - 대소문자에 숫자 및 특수문자를 포함하여 길게 만드세요. - “password”처럼 명백한 단어나 “abc”, “123 같은 문자나 숫자 순서는 피합니다. - 온라인에서 찾을 수 있는 개인 정보는 사용하지 마세요. 패스프레이즈를 사용하든 암호를 사용하든, 다른 곳에서 재사용하지 마세요. - 동료와 공유하지 마세요. - 다중 인증을 활성화합니다. - 전용 암호 관리자를 사용합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5_시스템에 대한 보안 액세스	모든 사람에게 암호 사용을 권장하세요. 이때 암호는 셋 이상의 자주 쓰이는 무작위 단어를 하나의 문구로 합쳐 기억하기 쉬우면서 안전한, 아주 좋은 조합입니다. 일반적인 암호를 선택하는 경우: - 대소문자에 숫자 및 특수문자를 포함하여 길게 만드세요. - “password”처럼 명백한 단어나 “abc”, “123 같은 문자나 숫자 순서는 피합니다. - 온라인에서 찾을 수 있는 개인 정보는 사용하지 마세요. 패스프레이즈를 사용하든 암호를 사용하든, 다른 곳에서 재사용하지 마세요. - 동료와 공유하지 마세요. - 다중 인증을 활성화합니다. - 전용 암호 관리자를 사용합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
5_시스템에 대한 보안 액세스	모든 사람에게 암호 사용을 권장하세요. 이때 암호는 셋 이상의 자주 쓰이는 무작위 단어를 하나의 문구로 합쳐 기억하기 쉬우면서 안전한, 아주 좋은 조합입니다. 일반적인 암호를 선택하는 경우: - 대소문자에 숫자 및 특수문자를 포함하여 길게 만드세요. - “password”처럼 명백한 단어나 “abc”, “123 같은 문자나 숫자 순서는 피합니다. - 온라인에서 찾을 수 있는 개인 정보는 사용하지 마세요. 패스프레이즈를 사용하든 암호를 사용하든, 다른 곳에서 재사용하지 마세요. - 동료와 공유하지 마세요. - 다중 인증을 활성화합니다. - 전용 암호 관리자를 사용합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 소프트웨어를 패치하고 최신 상태로 유지	중앙 집중식 플랫폼을 사용하여 패치를 관리하는 것이 이상적입니다. SME에게는 다음을 적극 권장합니다. - 모든 소프트웨어를 정기적으로 업데이트하세요. - 가능하면 자동 업데이트를 켜세요. - 수동 업데이트가 필요한 소프트웨어 및 하드웨어를 식별하세요. - 모바일 및 IoT 디바이스를 고려하세요.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
6_디바이스 보안: 소프트웨어를 패치하고 최신 상태로 유지	중앙 집중식 플랫폼을 사용하여 패치를 관리하는 것이 이상적입니다. SME에게는 다음을 적극 권장합니다. - 모든 소프트웨어를 정기적으로 업데이트하세요. - 가능하면 자동 업데이트를 켜세요. - 수동 업데이트가 필요한 소프트웨어 및 하드웨어를 식별하세요. - 모바일 및 IoT 디바이스를 고려하세요.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 소프트웨어를 패치하고 최신 상태로 유지	중앙 집중식 플랫폼을 사용하여 패치를 관리하는 것이 이상적입니다. SME에게는 다음을 적극 권장합니다. - 모든 소프트웨어를 정기적으로 업데이트하세요. - 가능하면 자동 업데이트를 켜세요. - 수동 업데이트가 필요한 소프트웨어 및 하드웨어를 식별하세요. - 모바일 및 IoT 디바이스를 고려하세요.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 소프트웨어를 패치하고 최신 상태로 유지	중앙 집중식 플랫폼을 사용하여 패치를 관리하는 것이 이상적입니다. SME에게는 다음을 적극 권장합니다. - 모든 소프트웨어를 정기적으로 업데이트하세요. - 가능하면 자동 업데이트를 켜세요. - 수동 업데이트가 필요한 소프트웨어 및 하드웨어를 식별하세요. - 모바일 및 IoT 디바이스를 고려하세요.	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. AWS Fargate 플랫폼 버전에 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.
6_디바이스 보안: 소프트웨어를 패치하고 최신 상태로 유지	중앙 집중식 플랫폼을 사용하여 패치를 관리하는 것이 이상적입니다. SME에게는 다음을 적극 권장합니다. - 모든 소프트웨어를 정기적으로 업데이트하세요. - 가능하면 자동 업데이트를 켜세요. - 수동 업데이트가 필요한 소프트웨어 및 하드웨어를 식별하세요. - 모바일 및 IoT 디바이스를 고려하세요.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 소프트웨어를 패치하고 최신 상태로 유지	중앙 집중식 플랫폼을 사용하여 패치를 관리하는 것이 이상적입니다. SME에게는 다음을 적극 권장합니다. - 모든 소프트웨어를 정기적으로 업데이트하세요. - 가능하면 자동 업데이트를 켜세요. - 수동 업데이트가 필요한 소프트웨어 및 하드웨어를 식별하세요. - 모바일 및 IoT 디바이스를 고려하세요.	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 소프트웨어를 패치하고 최신 상태로 유지	중앙 집중식 플랫폼을 사용하여 패치를 관리하는 것이 이상적입니다. SME에게는 다음을 적극 권장합니다. - 모든 소프트웨어를 정기적으로 업데이트하세요. - 가능하면 자동 업데이트를 켜세요. - 수동 업데이트가 필요한 소프트웨어 및 하드웨어를 식별하세요. - 모바일 및 IoT 디바이스를 고려하세요.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	codebuild-project-s3-logs-encrypted	저장 시 민감한 데이터를 보호하려면 Amazon S3에 저장된 your AWS CodeBuild 로그에 대해 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elasticsearch Service(Amazon ES) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	elasticsearch-node-to-node-encryption-check	Amazon Elasticsearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	opensearch-https-required	민감한 데이터가 존재할 수 있고 전송 중 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인 연결에 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Kinesis Streams에 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6_디바이스 보안: 암호화	데이터를 암호화하여 보호합니다. SME는 노트북, 스마트폰, 태블릿 같은 모바일 디바이스에 저장된 데이터를 암호화해야 합니다. 호텔 또는 공항 WiFi 네트워크 같은 공용 네트워크를 통해 전송되는 데이터의 경우 가상 프라이빗 네트워크(VPN)를 적용하거나 SSL/TLS 프로토콜을 사용하는 보안 연결을 통해 웹 사이트에 액세스하여 데이터를 암호화해야 합니다. 자체 웹 사이트가 인터넷을 통해 전송되는 클라이언트 데이터를 보호할 수 있는 적절한 암호화 기술을 적용하고 있는지 확인하세요.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 방화벽 사용	방화벽은 네트워크로 들어오고 나가는 트래픽을 관리하며 SME 시스템을 보호하는 데 중요한 도구입니다. 모든 중요 시스템을 보호하려면 방화벽을 배포해야 하며, 특히 인터넷으로부터 SME 네트워크를 보호하려면 방화벽을 사용해야 합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 방화벽 사용	방화벽은 네트워크로 들어오고 나가는 트래픽을 관리하며 SME 시스템을 보호하는 데 중요한 도구입니다. 모든 중요 시스템을 보호하려면 방화벽을 배포해야 하며, 특히 인터넷으로부터 SME 네트워크를 보호하려면 방화벽을 사용해야 합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 방화벽 사용	방화벽은 네트워크로 들어오고 나가는 트래픽을 관리하며 SME 시스템을 보호하는 데 중요한 도구입니다. 모든 중요 시스템을 보호하려면 방화벽을 배포해야 하며, 특히 인터넷으로부터 SME 네트워크를 보호하려면 방화벽을 사용해야 합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 방화벽 사용	방화벽은 네트워크로 들어오고 나가는 트래픽을 관리하며 SME 시스템을 보호하는 데 중요한 도구입니다. 모든 중요 시스템을 보호하려면 방화벽을 배포해야 하며, 특히 인터넷으로부터 SME 네트워크를 보호하려면 방화벽을 사용해야 합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 방화벽 사용	방화벽은 네트워크로 들어오고 나가는 트래픽을 관리하며 SME 시스템을 보호하는 데 중요한 도구입니다. 모든 중요 시스템을 보호하려면 방화벽을 배포해야 하며, 특히 인터넷으로부터 SME 네트워크를 보호하려면 방화벽을 사용해야 합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
7_네트워크 보안: 방화벽 사용	방화벽은 네트워크로 들어오고 나가는 트래픽을 관리하며 SME 시스템을 보호하는 데 중요한 도구입니다. 모든 중요 시스템을 보호하려면 방화벽을 배포해야 하며, 특히 인터넷으로부터 SME 네트워크를 보호하려면 방화벽을 사용해야 합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 방화벽 사용	방화벽은 네트워크로 들어오고 나가는 트래픽을 관리하며 SME 시스템을 보호하는 데 중요한 도구입니다. 모든 중요 시스템을 보호하려면 방화벽을 배포해야 하며, 특히 인터넷으로부터 SME 네트워크를 보호하려면 방화벽을 사용해야 합니다.	netfw-policy-rule-group-associated	AWS Network Firewall 정책은 방화벽이 Amazon VPC에서 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하여 패킷과 트래픽 흐름을 필터링하고 기본 트래픽 처리를 정의합니다.
7_네트워크 보안: 방화벽 사용	방화벽은 네트워크로 들어오고 나가는 트래픽을 관리하며 SME 시스템을 보호하는 데 중요한 도구입니다. 모든 중요 시스템을 보호하려면 방화벽을 배포해야 하며, 특히 인터넷으로부터 SME 네트워크를 보호하려면 방화벽을 사용해야 합니다.	netfw-stateless-rule-group-not-empty	AWS Network Firewall 규칙 그룹에는 방화벽이 VPC에서 트래픽을 처리하는 방법을 정의하는 규칙이 포함되어 있습니다. 방화벽 정책에 있는 빈 상태 비저장 규칙 그룹은 트래픽을 처리하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 방화벽 사용	방화벽은 네트워크로 들어오고 나가는 트래픽을 관리하며 SME 시스템을 보호하는 데 중요한 도구입니다. 모든 중요 시스템을 보호하려면 방화벽을 배포해야 하며, 특히 인터넷으로부터 SME 네트워크를 보호하려면 방화벽을 사용해야 합니다.	waf-regional-rule-not-empty	AWS WAF에 비어 있지 않은 규칙이 있는지 확인합니다. 조건이 없는 규칙에는 의도하지 않은 동작이 발생할 수 있습니다.
7_네트워크 보안: 방화벽 사용	방화벽은 네트워크로 들어오고 나가는 트래픽을 관리하며 SME 시스템을 보호하는 데 중요한 도구입니다. 모든 중요 시스템을 보호하려면 방화벽을 배포해야 하며, 특히 인터넷으로부터 SME 네트워크를 보호하려면 방화벽을 사용해야 합니다.	waf-regional-rulegroup-not-empty	AWS WAF에 비어 있지 않은 규칙 그룹이 있는지 확인합니다. 규칙 그룹이 비어 있으면 의도하지 않은 동작이 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 방화벽 사용	방화벽은 네트워크로 들어오고 나가는 트래픽을 관리하며 SME 시스템을 보호하는 데 중요한 도구입니다. 모든 중요 시스템을 보호하려면 방화벽을 배포해야 하며, 특히 인터넷으로부터 SME 네트워크를 보호하려면 방화벽을 사용해야 합니다.	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	elasticsearch-logs-to-cloudwatch	Amazon Elasticsearch 서비스 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7_네트워크 보안: 원격 액세스 솔루션 검토	SME는 모든 원격 액세스 도구를 정기적으로 검토하여 안전한지 확인해야 합니다. 특히: - 모든 원격 액세스 소프트웨어가 패치되고 최신 버전인지 확인하세요. - 의심스러운 지리적 위치 또는 특정 IP 주소의 원격 액세스를 제한합니다. - 직원이 업무에 필요한 시스템과 컴퓨터에만 원격으로 액세스할 수 있도록 제한합니다. - 원격 액세스에 강력한 암호를 적용하고 가능한 경우 다중 인증을 활성화합니다. - 의심스러운 공격이나 비정상적으로 의심스러운 활동을 경고할 수 있도록 모니터링 및 경고가 활성화되어 있어야 합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9_보안 백업	키 구성을 복구하려면 백업을 유지해야 합니다. 백업은 랜섬웨어 공격과 같은 재해로부터 효과적으로 복구하는 방법이기 때문입니다. 다음과 같은 백업 규칙을 적용해야 합니다. - 백업은 정기적으로 수행되고 가능하면 자동화됩니다. - 백업은 SME의 프로덕션 환경과 별도로 보관됩니다. - 백업은 암호화됩니다(특히 두 위치 간에 이동할 경우). - 백업에서 데이터를 정기적으로 복원하는 기능을 테스트합니다. 전체 복원을 처음부터 끝까지 정기적으로 테스트하는 것이 가장 좋습니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11_안전한 온라인 사이트	SME는 온라인 웹 사이트를 안전한 방식으로 구성 및 유지 관리하고 신용 카드 데이터와 같은 개인 데이터 또는 금융 세부 정보를 적절하게 보호해야 합니다. 이를 위해서는 웹사이트에 대해 정기적인 보안 테스트를 실시하여 잠재적인 보안 취약점을 식별하고 사이트가 적절하게 유지 관리 및 업데이트되고 있는지 정기적으로 검토해야 합니다.	vuln-management-plan-exists(프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 프로세스를 공식적으로 정의하려면 취약성 관리 계획을 개발하고 구현해야 합니다.

템플릿

템플릿은 GitHub: SME를 위한 ENISA 사이버 보안 가이드 운영 모범 사례에서 확인할 수 있습니다.

Esquema Nacional de Seguridad(ENS) Low 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Spain Esquema Nacional de Seguridad(ENS) Low 프레임워크 제어와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 Spain ENS Low 제어와 관련이 있습니다. Spain ENS 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 샘플 적합성 팩 템플릿에는 2020/10/23에 마지막으로 업데이트된 Spain ENS Low 프레임워크 내의 제어에 대한 매핑이 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간

제어 ID	AWS 구성 규칙	지침
		로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한, 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.
Anexo II 4.1.2.a); b); c)	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
Anexo II 4.1.2.b)	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.b)	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.
Anexo II 4.1.2.b)	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.1.a)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
Anexo II 4.2.1.a); b)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Anexo II 4.2.4	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.5	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.5.BAJO.a)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.5.BAJO.c)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.BAJO.c)	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.1	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
Anexo II 4.3.1	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.
Anexo II 4.3.1	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.1	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
Anexo II 4.3.2.b)	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
Anexo II 4.3.2.b)	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
Anexo II 4.3.2.b)	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
Anexo II 4.3.2.b)	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
Anexo II 4.3.4.c)	vuln-management-plan-exists (프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 프로세스를 공식적으로 정의하려면 취약성 관리 계획을 개발하고 구현해야 합니다. 여기에는 취약성 관리 도구, 환경 검사 주기, 역할 및 책임이 포함될 수 있습니다.
Anexo II 4.2.7.BAJO	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
Anexo II 4.2.7.BAJO	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
Anexo II 4.2.7.BAJO	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
Anexo II 4.2.7.BAJO	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
Anexo II 4.2.7.BAJO	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
Anexo II 4.2.7.BAJO	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Anexo II 4.2.7.BAJO	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
Anexo II 4.2.7.BAJO	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
Anexo II 5.2.3	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 직원들에게 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 교육합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.3.BAJO.a)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
Anexo II 5.7.3	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
Anexo II 5.7.3	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
Anexo II 5.7.3	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 5.7.3	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
Anexo II 5.7.3	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
Anexo II 5.7.3	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약되었을 경우 모든 키에 삭제 예약이 되었는지 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.2	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
Anexo II 5.8.2	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
Art. 14.4	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
Art. 16	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
Art. 16	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Art. 16	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
Art. 20.2	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	AWS 구성 규칙	지침
Art. 20.2	vuln-management-plan-exists (프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 프로세스를 공식적으로 정의하려면 취약성 관리 계획을 개발하고 구현해야 합니다. 여기에는 취약성 관리 도구, 환경 검사 주기, 역할 및 책임이 포함될 수 있습니다.
Art. 21.1	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
Art. 21.1	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한, 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
Art. 21.1	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.
Art. 21.1	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.
Art. 21.1	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
Art. 21.1	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
Art. 21.1	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
Art. 21.1	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 병목 현상 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.
Art. 21.1	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.
Art. 21.1	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Art. 21.1	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
Art. 21.1	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
Art. 21.1	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
Art. 21.1	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
Art. 21.1	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없어야 합니다. 이렇게 하면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
Art. 22	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 공개 SSM 문서에는 계정, 리소스 및 내부 프로세스에 대한 정보가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Art. 22	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Art. 22	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
Art. 22	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
Art. 22	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
Art. 22	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Art. 22	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
Art. 22	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
Art. 22	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Art. 22	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Art. 22	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
Art. 22	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
Art. 23	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
Art. 23	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 23	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
Art. 23	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
Art. 23	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
Art. 23	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
Art. 23	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
Art. 23	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 23	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Art. 23	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
Art. 23	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.
Art. 25	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.
Art. 25	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Art. 25	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
Art. 25	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
Art. 25	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
Art. 25	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
Art. 25	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

템플릿

템플릿은 GitHub: Esquema Nacional de Seguridad(ENS) Low 운영 모범 사례에서 확인할 수 있습니다.

Esquema Nacional de Seguridad(ENS) Medium 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Spain Esquema Nacional de Seguridad(ENS) 중형 프레임워크 제어와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 Spain ENS Medium 제어와 관련이 있습니다. Spain ENS 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 샘플 적합성 팩 템플릿에는 2020/10/23에 마지막으로 업데이트된 Spain ENS Medium 프레임워크 내의 제어에 대한 매핑이 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감

제어 ID	AWS 구성 규칙	지침
		한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한, 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
Anexo II 4.1.2.b)	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.b)	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.
Anexo II 4.1.2.b)	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.1.a)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
Anexo II 4.2.1.a); 4.2.1.b)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Anexo II 4.2.4	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.5	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.5.a)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.5.c)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Anexo II 4.2.6.c)	엘라스틱 서치-로그-투-클라우드 워치	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.c)	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
Anexo II 4.2.6.c)	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.c)	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
Anexo II 4.2.6.c)	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
Anexo II 4.2.6.c)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.c)	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
Anexo II 4.2.6.c)	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
Anexo II 4.2.6.c)	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.c)	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
Anexo II 4.2.6.c)	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
Anexo II 4.2.7	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
Anexo II 4.2.7	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
Anexo II 4.3.1	ec2-security-group-attached-to-eni-periodic	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
Anexo II 4.3.1	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
Anexo II 4.3.1	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.1	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
Anexo II 4.3.1	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
Anexo II 4.3.2.b)	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
Anexo II 4.3.2.b)	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
Anexo II 4.3.2.b)	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
Anexo II 4.3.2.b)	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
Anexo II 4.3.4.c)	vuln-management-plan-exists (프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 프로세스를 공식적으로 정의하려면 취약성 관리 계획을 개발하고 구현해야 합니다. 여기에는 취약성 관리 도구, 환경 검사 주기, 역할 및 책임이 포함될 수 있습니다.
Anexo II 4.3.1	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
부록 II 4.3.7.a)	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되는지 확인하세요. 대응 계획을 업데이트하고 공식적으로 문서화하면 대응 담당자가 역할, 책임 및 사고 발생 시 따라야 할 프로세스를 이해하는 데 도움이 될 수 있습니다.
Anexo II 4.3.8	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.8	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
Anexo II 4.3.8	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.8	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
Anexo II 4.3.8	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
Anexo II 4.3.8	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.8	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
Anexo II 4.3.8	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
Anexo II 4.3.8	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.8	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
Anexo II 4.3.8	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
Anexo II 4.2.7.BAJO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.6.2	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
Anexo II 4.6.2	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
Anexo II 5.2.3	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 직원들에게 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 교육합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.2	엘라스틱서치-노드 암호화 검사	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.2	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 5.4.2	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.2	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.2	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
Anexo II 5.4.2	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 5.4.2	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.2	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Anexo II 5.4.3	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.3	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 5.4.3	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.3	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.3	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.3	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 5.4.3	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.3	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.3.a)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
Anexo II 5.7.3	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
Anexo II 5.7.3	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
Anexo II 5.7.3	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 5.7.3	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
Anexo II 5.7.3	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
Anexo II 5.7.3	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약되었을 경우 모든 키에 삭제 예약이 되었는지 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.2	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
Anexo II 5.8.2	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.3.b)	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
Anexo II 5.8.3.b)	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.3.b)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한, 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
Anexo II 5.8.3.b)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.
Anexo II 5.8.3.b)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.3.b)	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.
Anexo II 5.8.3.b)	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.3.b)	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.3.b)	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
Art. 14.4	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Art. 16	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
Art. 16	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 16	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	AWS 구성 규칙	지침
Art. 20.2	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
Art. 20.2	vuln-management-plan-exists (프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 프로세스를 공식적으로 정의하려면 취약성 관리 계획을 개발하고 구현해야 합니다. 여기에는 취약성 관리 도구, 환경 검사 주기, 역할 및 책임이 포함될 수 있습니다.
Art. 21.1	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
Art. 21.1	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한, 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
Art. 21.1	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.
Art. 21.1	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.
Art. 21.1	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
Art. 21.1	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
Art. 21.1	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
Art. 21.1	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 병목 현상 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.
Art. 21.1	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.
Art. 21.1	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Art. 21.1	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
Art. 21.1	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
Art. 21.1	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
Art. 21.1	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
Art. 21.1	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없어야 합니다. 이렇게 하면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
Art. 22	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 공개 SSM 문서에는 계정, 리소스 및 내부 프로세스에 대한 정보가 노출될 수 있습니다.
Art. 22	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Art. 22	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Art. 22	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
Art. 22	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
Art. 22	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
Art. 22	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
Art. 22	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Art. 22	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
Art. 22	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
Art. 22	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Art. 22	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Art. 22	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
Art. 22	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
Art. 23	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
Art. 23	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 23	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
Art. 23	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
Art. 23	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
Art. 23	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
Art. 23	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
Art. 23	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 23	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Art. 23	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
Art. 23	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Art. 24.1	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
Art. 24.2	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되는지 확인하세요. 대응 계획을 업데이트하고 공식적으로 문서화하면 대응 담당자가 역할, 책임 및 사고 발생 시 따라야 할 프로세스를 이해하는 데 도움이 될 수 있습니다.
Art. 25	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Art. 25	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Art. 25	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
Art. 25	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
Art. 25	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
Art. 25	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
Art. 25	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

템플릿

템플릿은 GitHub: Esquema Nacional de Seguridad(ENS) Medium 운영 모범 사례에서 확인할 수 있습니다.

Esquema Nacional de Seguridad(ENS) High 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Spain Esquema Nacional de Seguridad(ENS) High 프레임워크 제어와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 Spain ENS High 제어와 관련이 있습니다. Spain ENS 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 샘플 적합성 팩 템플릿에는 2021/07/09에 마지막으로 업데이트된 Spain ENS High 프레임워크 내의 제어에 대한 매핑이 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.1.ALTO	annual-risk-assessment-performed(프로세스 확인)	조직에 대한 연간 위험 평가를 수행합니다. 위험 평가는 식별된 위험 및/또는 취약성이 조직에 영향을 미칠 가능성과 영향을 파악하는 데 도움이 될 수 있습니다.
4.2.1.b)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를

제어 ID	AWS 구성 규칙	지침
		생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
4.2.5.ALTO.a)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한, 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
Anexo II 4.1.2.b)	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.1.2.b)	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.
Anexo II 4.1.2.b)	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.1.a)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Anexo II 4.2.4	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.5	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.5.BAJO.a)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.5.BAJO.c)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.ALTO.b)	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
Anexo II 4.2.6.ALTO.b)	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.ALTO.b)	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
Anexo II 4.2.6.ALTO.b)	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Anexo II 4.2.6.BAJO.c)	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
Anexo II 4.3.1	ec2-security-group-attached-to-eni-periodic	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
Anexo II 4.3.1	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
Anexo II 4.3.1	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.1	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
Anexo II 4.3.1	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
Anexo II 4.3.2.b)	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
Anexo II 4.3.2.b)	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
Anexo II 4.3.2.b)	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
Anexo II 4.3.2.b)	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
Anexo II 4.3.4.c)	vuln-management-plan-exists (프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 프로세스를 공식적으로 정의하려면 취약성 관리 계획을 개발하고 구현해야 합니다. 여기에는 취약성 관리 도구, 환경 검사 주기, 역할 및 책임이 포함될 수 있습니다.
Anexo II 4.3.1	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.7.MEDIA.a)	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되는지 확인하세요. 대응 계획을 업데이트하고 공식적으로 문서화하면 대응 담당자가 역할, 책임 및 사고 발생 시 따라야 할 프로세스를 이해하는 데 도움이 될 수 있습니다.
Anexo II 4.2.7.BAJO	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
Anexo II 4.2.7.BAJO	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
Anexo II 4.2.7.BAJO	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
Anexo II 4.2.7.BAJO	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
Anexo II 4.2.7.BAJO	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
Anexo II 4.2.7.BAJO	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.2.7.BAJO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Anexo II 4.2.7.BAJO	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
Anexo II 4.2.7.BAJO	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.8.MEDIO	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Anexo II 4.3.8.MEDIO	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.8.MEDIO	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
Anexo II 4.3.8.MEDIO	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
Anexo II 4.3.8.MEDIO	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.8.MEDIO	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
Anexo II 4.3.8.MEDIO	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
Anexo II 4.3.8.MEDIO	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.8.MEDIO	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.8.MEDIO	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
Anexo II 4.3.8.MEDIO	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
Anexo II 4.6.2.ALTO	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(구성 기본값: 30), daysMediumSev(구성 기본값: 7) 및 daysHighSev(구성 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
Anexo II 4.6.2.MEDIA	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
Anexo II 5.2.3	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 직원들에게 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 교육합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.2.4	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 직원들에게 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 교육합니다.
Anexo II 5.2.5	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 직원들에게 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 교육합니다.
Anexo II 5.4.2.MEDIO	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.2.MEDIO	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 5.4.2.MEDIO	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.2.MEDIO	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.2.MEDIO	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.2.MEDIO	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Anexo II 5.4.2.MEDIO	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.2.MEDIO	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.3.BAJO.a)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.3.MEDIO	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.3.MEDIO	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 5.4.3.MEDIO	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.3.MEDIO	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.3.MEDIO	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
Anexo II 5.4.3.MEDIO	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Anexo II 5.4.3.MEDIO	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.4.3.MEDIO	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
Anexo II 5.7.3	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
Anexo II 5.7.3	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
Anexo II 5.7.3	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Anexo II 5.7.3	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
Anexo II 5.7.3	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
Anexo II 5.7.3	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.7.3	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약되었을 경우 모든 키에 삭제 예약이 되었는지 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.2	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
Anexo II 5.8.2	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.3.MEDIO.b)	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
Anexo II 5.8.3.MEDIO.b)	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.3.MEDIO.b)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한, 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
Anexo II 5.8.3.MEDIO.b)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.
Anexo II 5.8.3.MEDIO.b)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.3.MEDIO.b)	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.
Anexo II 5.8.3.MEDIO.b)	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.3.MEDIO.b)	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Anexo II 5.8.3.MEDIO.b)	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
Art. 14.4	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
Art. 16	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	AWS 구성 규칙	지침
Art. 16	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Art. 16	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	Amazon Relational Database Service(RDS) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 Relational Database Management System(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
Art. 20.2	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	AWS 구성 규칙	지침
Art. 20.2	vuln-management-plan-exists (프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 프로세스를 공식적으로 정의하려면 취약성 관리 계획을 개발하고 구현해야 합니다. 여기에는 취약성 관리 도구, 환경 검사 주기, 역할 및 책임이 포함될 수 있습니다.
Art. 21.1	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
Art. 21.1	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한, 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
Art. 21.1	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.
Art. 21.1	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.
Art. 21.1	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
Art. 21.1	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
Art. 21.1	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
Art. 21.1	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 병목 현상 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.
Art. 21.1	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.
Art. 21.1	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Art. 21.1	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.
Art. 21.1	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
Art. 21.1	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
Art. 21.1	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
Art. 21.1	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Art. 21.1	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Art. 21.1	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없어야 합니다. 이렇게 하면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
Art. 22	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 공개 SSM 문서에는 계정, 리소스 및 내부 프로세스에 대한 정보가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Art. 22	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Art. 22	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
Art. 22	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
Art. 22	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
Art. 22	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Art. 22	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS database instances can contain sensitive information and principles and access control is required for such accounts.
Art. 22	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
Art. 22	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Art. 22	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Art. 22	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
Art. 22	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Art. 22	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
Art. 23	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
Art. 23	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 23	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
Art. 23	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
Art. 23	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
Art. 23	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
Art. 23	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
Art. 23	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 23	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Art. 23	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
Art. 23	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Art. 24.2	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되는지 확인하세요. 대응 계획을 업데이트하고 공식적으로 문서화하면 대응 담당자가 역할, 책임 및 사고 발생 시 따라야 할 프로세스를 이해하는 데 도움이 될 수 있습니다.
Art. 24.1	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
Art. 25	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Art. 25	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Art. 25	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
Art. 25	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
Art. 25	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	AWS 구성 규칙	지침
Art. 25	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
Art. 25	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
Art. 25	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

템플릿

템플릿은 GitHub: Esquema Nacional de Seguridad(ENS) High 운영 모범 사례에서 확인할 수 있습니다.

FDA 타이틀 21 CFR 파트 11 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 미국 연방규정집(CFR) 파트 11의 타이틀 21과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 AWS Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 FDA Title 21 CFR Part 11 제어와 관련이 있습니다. FDA 타이틀 21 CFR 파트 11 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.1	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
11.1	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB

제어 ID	제어 설명	AWS 구성 규칙	지침
	송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다.		테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.1	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.1	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.1	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.1	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.1	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.1	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
11.1	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.1	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
11.1	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한, 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실될 수 있는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우 Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(a)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (a) 정확성, 신뢰성, 의도한 성능 일관성을 보장하기 위한 시스템 검증, 유효하지 않거나 변경된 기록을 식별하는 능력.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하기 때문에 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	ecr-private-lifecycle-policy-configured	Amazon Elastic Container Repository(ECR) 수명 주기 정책을 통해 리포지토리의 이미지에 대한 수명 주기 관리를 지정할 수 있습니다. 그러면 사용하지 않은 이미지를 자동으로 정리합니다. 예컨대 수명 또는 수를 바탕으로 이미지가 만료됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(c)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (c) 기록 보존 기간 내내 정확하고 즉시 검색할 수 있도록 기록을 보호하는 것.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(d)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (d) 승인된 개인으로 시스템 액세스를 제한하는 것.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	[api-gw-execution-logging-enabled](#)	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하기 때문에 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(e)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (e) 운영자 입력 및 전자 기록을 생성, 수정 또는 삭제하는 작업의 날짜와 시간을 독립적으로 기록하기 위한 안전한 컴퓨터 생성 타임 스탬프 감사 추적 사용. 기록 변경으로 인해 이전에 기록한 정보가 가려져서는 안 됩니다. 이러한 감사 기록 문서는 최소한 해당 전자 기록에 필요한 기간만큼 보관되어야 하며 기관 검토 및 복사에 사용할 수 있어야 합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(g)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (g) 승인된 개인만 시스템을 사용하고, 기록에 전자적으로 서명하고, 운영 또는 컴퓨터 시스템 입력 또는 출력 디바이스에 액세스하거나, 기록을 변경하거나, 당면한 작업을 수행할 수 있도록 보장하는 권한 확인 사용.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(h)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (h) 데이터 입력 소스 또는 운영 지침의 유효성을 적절하게 판단하는 디바이스(예: 터미널) 사용.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(h)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (h) 데이터 입력 소스 또는 운영 지침의 유효성을 적절하게 판단하는 디바이스(예: 터미널) 사용.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(h)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (h) 데이터 입력 소스 또는 운영 지침의 유효성을 적절하게 판단하는 디바이스(예: 터미널) 사용.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(i)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (i) 전자 기록/전자 서명 시스템을 개발, 유지 또는 사용하는 사람이 지정된 업무를 수행할 수 있는 교육, 훈련 및 경험을 갖추고 있는지 판단.	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 직원들에게 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 교육합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없어야 합니다. 이렇게 하면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 조치, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.10(k)	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 기밀성을 보장하고, 서명자가 서명된 기록을 원본이 아니라고 쉽게 부인할 수 없도록 설계된 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 다음이 포함되어야 합니다. (k) 다음을 포함한 시스템 문서에 대한 적절한 통제 사용: (1) 시스템 운영 및 유지보수를 위한 문서의 배포, 액세스 및 사용에 대한 적절한 통제. (2) 시스템 문서의 개발 및 수정을 시간 순서대로 문서화하는 감사 추적을 유지하기 위한 개정 및 변경 관리 절차.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	(a) 생체 인식을 기반으로 하지 않는 전자 서명은 다음을 준수해야 합니다. (1) 식별 코드와 암호 같은 두 가지 이상의 고유한 식별 구성 요소를 사용합니다. (i) 통제된 단일 연속 시스템 액세스 기간 동안 개인이 일련의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 첫 번째 서명을 실행해야 합니다. 후속 서명은 개인만 실행할 수 있고 해당 개인만 사용하도록 설계된 전자 서명 구성 요소를 하나 이상 사용하여 실행합니다. (ii) 개인이 통제된 단일 연속 시스템 액세스 기간 동안 수행되지 않은 하나 이상의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 각 서명을 실행합니다. (2) 원래 소유자만 사용할 수 있어야 합니다. (3) 원래 소유자가 아닌 다른 사람이 개인의 전자 서명을 사용하려는 경우 두 명 이상의 개인 협업이 필	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	요하도록 관리하고 실행해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	(a) 생체 인식을 기반으로 하지 않는 전자 서명은 다음을 준수해야 합니다. (1) 식별 코드와 암호 같은 두 가지 이상의 고유한 식별 구성 요소를 사용합니다. (i) 통제된 단일 연속 시스템 액세스 기간 동안 개인이 일련의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 첫 번째 서명을 실행해야 합니다. 후속 서명은 개인만 실행할 수 있고 해당 개인만 사용하도록 설계된 전자 서명 구성 요소를 하나 이상 사용하여 실행합니다. (ii) 개인이 통제된 단일 연속 시스템 액세스 기간 동안 수행되지 않은 하나 이상의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 각 서명을 실행합니다. (2) 원래 소유자만 사용할 수 있어야 합니다. (3) 원래 소유자가 아닌 다른 사람이 개인의 전자 서명을 사용하려는 경우 두 명 이상의 개인 협업이 필	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
	요하도록 관리하고 실행해야 합니다.		조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	(a) 생체 인식을 기반으로 하지 않는 전자 서명은 다음을 준수해야 합니다. (1) 식별 코드와 암호 같은 두 가지 이상의 고유한 식별 구성 요소를 사용합니다. (i) 통제된 단일 연속 시스템 액세스 기간 동안 개인이 일련의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 첫 번째 서명을 실행해야 합니다. 후속 서명은 개인만 실행할 수 있고 해당 개인만 사용하도록 설계된 전자 서명 구성 요소를 하나 이상 사용하여 실행합니다. (ii) 개인이 통제된 단일 연속 시스템 액세스 기간 동안 수행되지 않은 하나 이상의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 각 서명을 실행합니다. (2) 원래 소유자만 사용할 수 있어야 합니다. (3) 원래 소유자가 아닌 다른 사람이 개인의 전자 서명을 사용하려는 경우 두 명 이상의 개인 협업이 필	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	요하도록 관리하고 실행해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	(a) 생체 인식을 기반으로 하지 않는 전자 서명은 다음을 준수해야 합니다. (1) 식별 코드와 암호 같은 두 가지 이상의 고유한 식별 구성 요소를 사용합니다. (i) 통제된 단일 연속 시스템 액세스 기간 동안 개인이 일련의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 첫 번째 서명을 실행해야 합니다. 후속 서명은 개인만 실행할 수 있고 해당 개인만 사용하도록 설계된 전자 서명 구성 요소를 하나 이상 사용하여 실행합니다. (ii) 개인이 통제된 단일 연속 시스템 액세스 기간 동안 수행되지 않은 하나 이상의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 각 서명을 실행합니다. (2) 원래 소유자만 사용할 수 있어야 합니다. (3) 원래 소유자가 아닌 다른 사람이 개인의 전자 서명을 사용하려는 경우 두 명 이상의 개인 협업이 필	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
	요하도록 관리하고 실행해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	(a) 생체 인식을 기반으로 하지 않는 전자 서명은 다음을 준수해야 합니다. (1) 식별 코드와 암호 같은 두 가지 이상의 고유한 식별 구성 요소를 사용합니다. (i) 통제된 단일 연속 시스템 액세스 기간 동안 개인이 일련의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 첫 번째 서명을 실행해야 합니다. 후속 서명은 개인만 실행할 수 있고 해당 개인만 사용하도록 설계된 전자 서명 구성 요소를 하나 이상 사용하여 실행합니다. (ii) 개인이 통제된 단일 연속 시스템 액세스 기간 동안 수행되지 않은 하나 이상의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 각 서명을 실행합니다. (2) 원래 소유자만 사용할 수 있어야 합니다. (3) 원래 소유자가 아닌 다른 사람이 개인의 전자 서명을 사용하려는 경우 두 명 이상의 개인 협업이 필	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	요하도록 관리하고 실행해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	(a) 생체 인식을 기반으로 하지 않는 전자 서명은 다음을 준수해야 합니다. (1) 식별 코드와 암호 같은 두 가지 이상의 고유한 식별 구성 요소를 사용합니다. (i) 통제된 단일 연속 시스템 액세스 기간 동안 개인이 일련의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 첫 번째 서명을 실행해야 합니다. 후속 서명은 개인만 실행할 수 있고 해당 개인만 사용하도록 설계된 전자 서명 구성 요소를 하나 이상 사용하여 실행합니다. (ii) 개인이 통제된 단일 연속 시스템 액세스 기간 동안 수행되지 않은 하나 이상의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 각 서명을 실행합니다. (2) 원래 소유자만 사용할 수 있어야 합니다. (3) 원래 소유자가 아닌 다른 사람이 개인의 전자 서명을 사용하려는 경우 두 명 이상의 개인 협업이 필	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
	요하도록 관리하고 실행해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2	(a) 생체 인식을 기반으로 하지 않는 전자 서명은 다음을 준수해야 합니다. (1) 식별 코드와 암호 같은 두 가지 이상의 고유한 식별 구성 요소를 사용합니다. (i) 통제된 단일 연속 시스템 액세스 기간 동안 개인이 일련의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 첫 번째 서명을 실행해야 합니다. 후속 서명은 개인만 실행할 수 있고 해당 개인만 사용하도록 설계된 전자 서명 구성 요소를 하나 이상 사용하여 실행합니다. (ii) 개인이 통제된 단일 연속 시스템 액세스 기간 동안 수행되지 않은 하나 이상의 서명을 실행하는 경우 모든 전자 서명 구성 요소를 사용하여 각 서명을 실행합니다. (2) 원래 소유자만 사용할 수 있어야 합니다. (3) 원래 소유자가 아닌 다른 사람이 개인의 전자 서명을 사용하려는 경우 두 명 이상의 개인 협업이 필	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
	요하도록 관리하고 실행해야 합니다.		
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	codebuild-project-s3-logs-encrypted	저장 시 민감한 데이터를 보호하려면 Amazon S3에 저장된 your AWS CodeBuild 로그에 대해 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic File System(EFS)에서 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service(OpenSearch Service) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elastic Block Store(Amazon EBS)에서 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Kinesis Streams에 암호화를 활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.3	폐쇄형 시스템을 사용하여 전자 기록을 작성, 수정, 유지 또는 전송하는 사람은 전자 기록의 신뢰성, 무결성 및 적절한 경우 전자 기록의 생성 시점부터 수령 시점까지 기밀성을 보장하는 절차와 제어를 사용해야 합니다. 이러한 절차와 통제에는 11.10에 명시된 내용 뿐만 아니라 상황에 필요한 바에 따라 기록의 신뢰성, 무결성 및 기밀성을 보장하기 위한 문서 암호화 및 적절한 디지털 서명 표준 사용 등의 추가 조치가 포함되어야 합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.300(b)	암호와 함께 식별 코드를 사용하는 전자 서명을 사용하는 사람은 보안 및 무결성을 보장하기 위한 통제 수단을 사용해야 합니다. 이러한 통제에는 다음이 포함되어야 합니다. (b) 식별 코드 및 암호 발급을 정기적으로 점검, 리콜 또는 개정하도록 보장(예: 암호 노후화와 같은 이벤트 처리).	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.300(b)	암호와 함께 식별 코드를 사용하는 전자 서명을 사용하는 사람은 보안 및 무결성을 보장하기 위한 통제 수단을 사용해야 합니다. 이러한 통제에는 다음이 포함되어야 합니다. (b) 식별 코드 및 암호 발급을 정기적으로 점검, 리콜 또는 개정하도록 보장(예: 암호 노후화와 같은 이벤트 처리).	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.300(b)	암호와 함께 식별 코드를 사용하는 전자 서명을 사용하는 사람은 보안 및 무결성을 보장하기 위한 통제 수단을 사용해야 합니다. 이러한 통제에는 다음이 포함되어야 합니다. (b) 식별 코드 및 암호 발급을 정기적으로 점검, 리콜 또는 개정하도록 보장(예: 암호 노후화와 같은 이벤트 처리).	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
11.300(b)	암호와 함께 식별 코드를 사용하는 전자 서명을 사용하는 사람은 보안 및 무결성을 보장하기 위한 통제 수단을 사용해야 합니다. 이러한 통제에는 다음이 포함되어야 합니다. (b) 식별 코드 및 암호 발급을 정기적으로 점검, 리콜 또는 개정하도록 보장(예: 암호 노후화와 같은 이벤트 처리).	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.300(b)	암호와 함께 식별 코드를 사용하는 전자 서명을 사용하는 사람은 보안 및 무결성을 보장하기 위한 통제 수단을 사용해야 합니다. 이러한 통제에는 다음이 포함되어야 합니다. (b) 식별 코드 및 암호 발급을 정기적으로 점검, 리콜 또는 개정하도록 보장(예: 암호 노후화와 같은 이벤트 처리).	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
11.300(b)	암호와 함께 식별 코드를 사용하는 전자 서명을 사용하는 사람은 보안 및 무결성을 보장하기 위한 통제 수단을 사용해야 합니다. 이러한 통제에는 다음이 포함되어야 합니다. (b) 식별 코드 및 암호 발급을 정기적으로 점검, 리콜 또는 개정하도록 보장(예: 암호 노후화와 같은 이벤트 처리).	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.300(d)	암호와 함께 식별 코드를 사용하는 전자 서명을 사용하는 사람은 보안 및 무결성을 보장하기 위한 통제 수단을 사용해야 합니다. 이러한 통제에는 다음이 포함되어야 합니다. (d) 암호 및/또는 식별 코드의 무단 사용을 방지하고 무단 사용 시도를 즉각적이고 긴급하게 탐지하여 시스템 보안 부서 및 적절한 경우 조직 경영진에게 보고하기 위한 트랜잭션 보호 장치의 사용.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.300(d)	암호와 함께 식별 코드를 사용하는 전자 서명을 사용하는 사람은 보안 및 무결성을 보장하기 위한 통제 수단을 사용해야 합니다. 이러한 통제에는 다음이 포함되어야 합니다. (d) 암호 및/또는 식별 코드의 무단 사용을 방지하고 무단 사용 시도를 즉각적이고 긴급하게 탐지하여 시스템 보안 부서 및 적절한 경우 조직 경영진에게 보고하기 위한 트랜잭션 보호 장치의 사용.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.300(d)	암호와 함께 식별 코드를 사용하는 전자 서명을 사용하는 사람은 보안 및 무결성을 보장하기 위한 통제 수단을 사용해야 합니다. 이러한 통제에는 다음이 포함되어야 합니다. (d) 암호 및/또는 식별 코드의 무단 사용을 방지하고 무단 사용 시도를 즉각적이고 긴급하게 탐지하여 시스템 보안 부서 및 적절한 경우 조직 경영진에게 보고하기 위한 트랜잭션 보호 장치의 사용.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.300(d)	암호와 함께 식별 코드를 사용하는 전자 서명을 사용하는 사람은 보안 및 무결성을 보장하기 위한 통제 수단을 사용해야 합니다. 이러한 통제에는 다음이 포함되어야 합니다. (d) 암호 및/또는 식별 코드의 무단 사용을 방지하고 무단 사용 시도를 즉각적이고 긴급하게 탐지하여 시스템 보안 부서 및 적절한 경우 조직 경영진에게 보고하기 위한 트랜잭션 보호 장치의 사용.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

템플릿

템플릿은 GitHub: FDA 타이틀 21 CFR 파트 11 운영 모범 사례에서 확인할 수 있습니다.

FedRAMP(Low) 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 연방 위험 및 권한 부여 관리 프로그램(FedRAMP) Low Baseline Controls와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 FedRAMP 제어와 관련이 있습니다. FedRAMP 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
AC-2	계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하

제어 ID	제어 설명	AWS 구성 규칙	지침
			면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
AC-2	계정 관리	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-2	계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AC-2	계정 관리	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AC-2	계정 관리	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AC-2	계정 관리	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2	계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2	계정 관리	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2	계정 관리	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-2	계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AC-2	계정 관리	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AC-3	액세스 적용	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
AC-3	액세스 적용	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
AC-3	액세스 적용	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-3	액세스 적용	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
AC-3	액세스 적용	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	액세스 적용	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	액세스 적용	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	액세스 적용	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-3	액세스 적용	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-3	액세스 적용	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AC-3	액세스 적용	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	액세스 적용	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC-3	액세스 적용	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-3	액세스 적용	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 적용	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
AC-17	원격 액세스	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
AC-17	원격 액세스	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-17	원격 액세스	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-17	원격 액세스	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
AC-17	원격 액세스	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AC-17	원격 액세스	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-17	원격 액세스	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-17	원격 액세스	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC-17	원격 액세스	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-17	원격 액세스	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC-17	원격 액세스	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17	원격 액세스	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
AU-2	감사 이벤트	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	감사 이벤트	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	감사 이벤트	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AU-2	감사 이벤트	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	감사 이벤트	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-2	감사 이벤트	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-2	감사 이벤트	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	감사 이벤트	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AU-2	감사 이벤트	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	감사 이벤트	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	감사 이벤트	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-2	감사 이벤트	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AU-3	감사 기록 내용	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-3	감사 기록 내용	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-3	감사 기록 내용	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AU-3	감사 기록 내용	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-3	감사 기록 내용	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6	감사 검토, 분석 및 보고	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
AU-6	감사 검토, 분석 및 보고	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하기 때문에 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6	감사 검토, 분석 및 보고	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6	감사 검토, 분석 및 보고	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6	감사 검토, 분석 및 보고	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
AU-6	감사 검토, 분석 및 보고	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-6	감사 검토, 분석 및 보고	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6	감사 검토, 분석 및 보고	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-6	감사 검토, 분석 및 보고	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6	감사 검토, 분석 및 보고	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6	감사 검토, 분석 및 보고	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
AU-6	감사 검토, 분석 및 보고	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6	감사 검토, 분석 및 보고	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6	감사 검토, 분석 및 보고	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6	감사 검토, 분석 및 보고	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-6	감사 검토, 분석 및 보고	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9	감사 정보 보호	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
AU-9	감사 정보 보호	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9	감사 정보 보호	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
AU-9	감사 정보 보호	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9	감사 정보 보호	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
AU-11	감사 기록 보존	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하기 때문에 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 작업	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 작업	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 작업	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AU-12	감사 작업	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	감사 작업	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-12	감사 작업	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU–12	감사 작업	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	감사 작업	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AU–12	감사 작업	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 작업	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 작업	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-12	감사 작업	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.
CA-7	지속적인 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	securityhub-enabled	AWS Security Hub 는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 확장 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CA-7	지속적인 모니터링	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
CA-7	지속적인 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CA-7	지속적인 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
CM-2	베이스라인 구성	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
CM-2	베이스라인 구성	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM-2	베이스라인 구성	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM-2	베이스라인 구성	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM-2	베이스라인 구성	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
CM-2	베이스라인 구성	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM-2	베이스라인 구성	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CM-2	베이스라인 구성	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CM-2	베이스라인 구성	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
CM-2	베이스라인 구성	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
CM-2	베이스라인 구성	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	베이스라인 구성	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CM-2	베이스라인 구성	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-7	최소 자릿수	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
CM-7	최소 자릿수	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-7	최소 자릿수	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8	정보 시스템 구성 요소 인벤토리	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8	정보 시스템 구성 요소 인벤토리	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
CM-8	정보 시스템 구성 요소 인벤토리	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8	정보 시스템 구성 요소 인벤토리	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CP-9	정보 시스템 백업	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템 백업	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템 백업	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9	정보 시스템 백업	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템 백업	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9	정보 시스템 백업	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템 백업	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9	정보 시스템 백업	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템 백업	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
CP-9	정보 시스템 백업	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템 백업	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
CP-9	정보 시스템 백업	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템 백업	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-9	정보 시스템 백업	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	정보 시스템 복구 및 재구성	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	정보 시스템 복구 및 재구성	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
CP-10	정보 시스템 복구 및 재구성	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	정보 시스템 복구 및 재구성	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CP-10	정보 시스템 복구 및 재구성	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
CP-10	정보 시스템 복구 및 재구성	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CP-10	정보 시스템 복구 및 재구성	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-10	정보 시스템 복구 및 재구성	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	정보 시스템 복구 및 재구성	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2	식별 및 인증(기관 사용자)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IA-2	식별 및 인증(기관 사용자)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
IA-2	식별 및 인증(기관 사용자)	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2	식별 및 인증(기관 사용자)	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2	식별 및 인증(기관 사용자)	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA-2	식별 및 인증(기관 사용자)	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-5	인증자 관리	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-5	인증자 관리	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IR-4	인시던트 처리	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4	인시던트 처리	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
IR-4	인시던트 처리	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4	인시던트 처리	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4	인시던트 처리	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-6	인시던트 보고	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
IR-6	인시던트 보고	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-6	인시던트 보고	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-7	인시던트 대응 지원	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
IR-7	인시던트 대응 지원	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-7	인시던트 대응 지원	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5	취약성 스캔	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5	취약성 스캔	securityhub-enabled	AWS Security Hub 는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5	취약성 스캔	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SA-3	시스템 개발 수명 주기	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-3	시스템 개발 수명 주기	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
SA-3	시스템 개발 수명 주기	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	서비스 거부 보호	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
SC-5	서비스 거부 보호	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	서비스 거부 보호	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	서비스 거부 보호	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기 및 쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
SC-5	서비스 거부 보호	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	서비스 거부 보호	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
SC-5	서비스 거부 보호	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	서비스 거부 보호	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
SC-5	서비스 거부 보호	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	서비스 거부 보호	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	서비스 거부 보호	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
SC-5	서비스 거부 보호	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	서비스 거부 보호	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
SC-7	경계 보호	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서에는 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
SC-7	경계 보호	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
SC-7	경계 보호	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7	경계 보호	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7	경계 보호	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
SC-7	경계 보호	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7	경계 보호	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
SC-7	경계 보호	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
SC-7	경계 보호	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-12	암호 키 설정 및 관리	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
SC-12	암호 키 설정 및 관리	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
SC-12	암호 키 설정 및 관리	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
SC-13	암호화 보호	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	암호화 보호	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	암호화 보호	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2	결함 수정	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2	결함 수정	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
SI-2	결함 수정	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2	결함 수정	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
SI-3	결함 수정	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3	결함 수정	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
SI-3	결함 수정	ecs-task-definition-memory-hard-limit	Amazon Elastic Container Service(ECS) 컨테이너에 사용할 수 있는 최대 메모리를 제한하면 컨테이너에 악의적으로 액세스하는 경우 리소스 사용이 남용되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4	정보 시스템 모니터링	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 소비할 수 있습니다.
SI-4	정보 시스템 모니터링	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4	정보 시스템 모니터링	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4	정보 시스템 모니터링	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4	정보 시스템 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4	정보 시스템 모니터링	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
SI-4	정보 시스템 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4	정보 시스템 모니터링	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
SI-4	정보 시스템 모니터링	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4	정보 시스템 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI-4	정보 시스템 모니터링	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4	정보 시스템 모니터링	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4	정보 시스템 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-5	보안 경고, 권고 및 지침	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-5	보안 경고, 권고 및 지침	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SI-5	보안 경고, 권고 및 지침	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-5	보안 경고, 권고 및 지침	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 처리 및 보존	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 처리 및 보존	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 처리 및 보존	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
SI-12	정보 처리 및 보존	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 처리 및 보존	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	정보 처리 및 보존	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 처리 및 보존	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	정보 처리 및 보존	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 처리 및 보존	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	정보 처리 및 보존	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 처리 및 보존	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
SI-12	정보 처리 및 보존	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 처리 및 보존	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
SI-12	정보 처리 및 보존	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-16	메모리 보호	ecs-task-definition-memory-hard-limit	Amazon Elastic Container Service(ECS) 컨테이너에 사용할 수 있는 최대 메모리를 제한하면 컨테이너에 악의적으로 액세스하는 경우 리소스 사용이 남용되는 것을 방지할 수 있습니다.

템플릿

템플릿은 GitHub: FedRAMP(Low) 운영 모범 사례에서 확인할 수 있습니다.

FedRAMP(Moderate) 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Federal Risk and Authorization Management Program(FedRAMP)과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 FedRAMP 제어와 관련이 있습니다. FedRAMP 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 적합성 팩은 Payment Card Industry Qualified Security Assessors(QSAs), HITRUST Certified Common Security Framework Practitioners(CCSFPs) 및 다양한 산업 프레임워크에 대한 지침과 평가를 제공하도록 인증된 규정 준수 전문가로 구성된 팀AWS 인 AWS Security Assurance Services LLC(AWS SAS)에서 검증되었습니다.SAS 전문가는 고객이 FedRAMP 제어의 하위 집합에 맞게이 적합성 팩을 설계했습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및

제어 ID	제어 설명	AWS 구성 규칙	지침
			AWS 파트너 솔루션이 있습니다.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(3)	정보 시스템은 90일이 지나면 사용자의 비활성 계정을 자동으로 비활성화합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2(3)	정보 시스템은 90일이 지나면 사용자의 비활성 계정을 자동으로 비활성화합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자를 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자를 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자를 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자를 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자를 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자를 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(12)(a)	조직: a. 정보 시스템 계정의 [할당: 조직에서 정의한 비정형 용도] 활동을 모니터링합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(12)(a)	조직: a. 정보 시스템 계정의 [할당: 조직에서 정의한 비정형 용도] 활동을 모니터링합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-6(10)	정보 시스템은 권한이 없는 사용자가 구현된 보안 보호 장치 및 대응 조치를 비활성화, 우회 또는 변경하는 것을 포함하는 권한 있는 기능을 실행하는 것을 방지합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(10)	정보 시스템은 권한이 없는 사용자가 구현된 보안 보호 장치 및 대응 조치를 비활성화, 우회 또는 변경하는 것을 포함하는 권한 있는 기능을 실행하는 것을 방지합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-6(10)	정보 시스템은 권한이 없는 사용자가 구현된 보안 보호 장치 및 대응 조치를 비활성화, 우회 또는 변경하는 것을 포함하는 권한 있는 기능을 실행하는 것을 방지합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-7(1)	정보 시스템은 [할당: 감사 기록 내 조직이 정의한 감사 필드]를 기반으로 관심 이벤트에 대한 감사 기록을 처리할 수 있는 기능을 제공합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-7(1)	정보 시스템은 [할당: 감사 기록 내 조직이 정의한 감사 필드]를 기반으로 관심 이벤트에 대한 감사 기록을 처리할 수 있는 기능을 제공합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9(2)	정보 시스템은 감사 기록을 최소한 매주 감사 대상 시스템 또는 구성 요소와 물리적으로 다른 시스템 또는 시스템 구성 요소에 백업합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
AU-9(2)	정보 시스템은 감사 기록을 최소한 매주 감사 대상 시스템 또는 구성 요소와 물리적으로 다른 시스템 또는 시스템 구성 요소에 백업합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9	정보 시스템은 감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
AU-9	정보 시스템은 감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9	정보 시스템은 감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
AU-11	조직은 보안 사고에 대한 사후 조사를 지원하고 규정 및 조직의 정보 보존 요구 사항을 충족하기 위해 최소 90일 동안 감사 기록을 보관합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 강화된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-7(a)	조직: a. 필수 기능만 제공하도록 정보 시스템을 구성합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
CM-7(a)	조직: a. 필수 기능만 제공하도록 정보 시스템을 구성합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-7(a)	조직: a. 필수 기능만 제공하도록 정보 시스템을 구성합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(1)	조직은 구성 요소 설치, 제거 및 정보 시스템 업데이트의 필수 부분으로 정보 시스템 구성 요소 인벤토리를 업데이트합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(1)	조직은 구성 요소 설치, 제거 및 정보 시스템 업데이트의 필수 부분으로 정보 시스템 구성 요소 인벤토리를 업데이트합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(3)(a)	조직: a. 탐지 시 최대 5분 지연되는 자동 메커니즘을 사용하여 정보 시스템 내에 승인되지 않은 하드웨어, 소프트웨어 및 펌웨어 구성 요소가 있는지 탐지하는 자동 메커니즘을 지속적으로 적용합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(3)(a)	조직: a. 탐지 시 최대 5분 지연되는 자동 메커니즘을 사용하여 정보 시스템 내에 승인되지 않은 하드웨어, 소프트웨어 및 펌웨어 구성 요소가 있는지 탐지하는 자동 메커니즘을 지속적으로 적용합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
CM-8(3)(a)	조직: a. 탐지 시 최대 5분 지연되는 자동 메커니즘을 사용하여 정보 시스템 내에 승인되지 않은 하드웨어, 소프트웨어 및 펌웨어 구성 요소가 있는지 탐지하는 자동 메커니즘을 지속적으로 적용합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(3)(a)	조직: a. 탐지 시 최대 5분 지연되는 자동 메커니즘을 사용하여 정보 시스템 내에 승인되지 않은 하드웨어, 소프트웨어 및 펌웨어 구성 요소가 있는지 탐지하는 자동 메커니즘을 지속적으로 적용합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(1)(2)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다. (2) 정보 시스템은 권한이 없는 계정에 대한 네트워크 액세스를 위해 다중 인증을 구현합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA-2(1)(2)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다. (2) 정보 시스템은 권한이 없는 계정에 대한 네트워크 액세스를 위해 다중 인증을 구현합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(1)(2)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다. (2) 정보 시스템은 권한이 없는 계정에 대한 네트워크 액세스를 위해 다중 인증을 구현합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(1)(2)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다. (2) 정보 시스템은 권한이 없는 계정에 대한 네트워크 액세스를 위해 다중 인증을 구현합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA-2(1)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(1)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(1)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA-2(1)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2	정보 시스템은 조직 사용자(또는 조직 사용자를 대신하여 활동하는 프로세스)를 고유하게 식별하고 인증합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IA-2	정보 시스템은 조직 사용자(또는 조직 사용자를 대신하여 활동하는 프로세스)를 고유하게 식별하고 인증합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-5(1)(a)(d)(e)	암호 기반 인증을 위한 정보 시스템: a. a. 최소한의 암호 복잡성 수준 강제[할당: 각 유형에 대한 최소 요구 사항을 포함하여 대소문자 구분, 문자 수, 대소문자 혼합, 숫자 및 특수 문자에 대한 조직에서 정의한 요구 사항] d. 암호의 최소 및 최대 수명 제한 적용[할당: 조직에서 정의한 최소 수명 및 최대 수명] 24회 생성에 암호 재사용을 금지합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-5(4)	조직에서는 자동화된 도구를 사용하여 암호 인증자가 [할당: 조직에서 정의한 요구 사항]을 충족할 만큼 충분히 강력한지 판단합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IA-5(7)	조직은 암호화되지 않은 정적 인증자가 애플리케이션이나 액세스 스크립트에 내장되거나 기능 키에 저장되지 않도록 합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-6(1)	조직은 자동화된 메커니즘을 사용하여 보안 인시던트를 보고하는 것을 지원합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
IR-6(1)	조직은 자동화된 메커니즘을 사용하여 보안 인시던트를 보고하는 것을 지원합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-6(1)	조직은 자동화된 메커니즘을 사용하여 보안 인시던트를 보고하는 것을 지원합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-7(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 대응 관련 정보 및 지원의 가용성을 높입니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
IR-7(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 대응 관련 정보 및 지원의 가용성을 높입니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-7(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 대응 관련 정보 및 지원의 가용성을 높입니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5(1)	조직은 검사할 정보 시스템 취약성을 즉시 업데이트할 수 있는 기능이 포함된 취약성 검사 도구를 사용합니다. 보충 지침: 새로운 취약성이 발견되고 발표되고 검사 방법이 개발되면 검사할 취약성을 즉시 업데이트해야 합니다. 이 업데이트 프로세스는 정보 시스템의 잠재적 취약성을 최대한 빨리 식별하고 해결하는 데 도움이 됩니다. 관련 규제 항목: SI-3, SI-7.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5(1)	조직은 검사할 정보 시스템 취약성을 즉시 업데이트할 수 있는 기능이 포함된 취약성 검사 도구를 사용합니다. 보충 지침: 새로운 취약성이 발견되고 발표되고 검사 방법이 개발되면 검사할 취약성을 즉시 업데이트해야 합니다. 이 업데이트 프로세스는 정보 시스템의 잠재적 취약성을 최대한 빨리 식별하고 해결하는 데 도움이 됩니다. 관련 규제 항목: SI-3, SI-7.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5(1)	조직은 검사할 정보 시스템 취약성을 즉시 업데이트할 수 있는 기능이 포함된 취약성 검사 도구를 사용합니다. 보충 지침: 새로운 취약성이 발견되고 발표되고 검사 방법이 개발되면 검사할 취약성을 즉시 업데이트해야 합니다. 이 업데이트 프로세스는 정보 시스템의 잠재적 취약성을 최대한 빨리 식별하고 해결하는 데 도움이 됩니다. 관련 규제 항목: SI-3, SI-7.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5	조직: a. 매월 [운영 체제/인프라, 월간 웹 애플리케이션 및 데이터베이스], 그리고 시스템/애플리케이션에 영향을 미칠 수 있는 새로운 취약성이 식별되고 보고되는 시점을 기준으로 정보 시스템 및 호스팅된 애플리케이션의 취약성을 검사합니다. b. 조직 b: 다음에 대한 표준을 사용하여 도구 간의 상호 운용성을 촉진하고 취약성 관리 프로세스의 일부를 자동화하는 취약성 스캔 도구 및 기법을 사용합니다. 1. 플랫폼, 소프트웨어 결함 및 부적절한 구성 열거 2. 체크리스트 및 테스트 절차 형식 지정 3. 취약성 영향 측정 조직 c: 취약성 검사 보고서 및 보안 통제 평가 결과를 분석합니다. 합법적인 취약성을 해결합니다. 조직의 위험 평가에 따라 발견일로부터 30일 이내에 완화된 고위험 취약성, 발견일로부터 90일 이내에 완화된 중간 위험 취약	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	성, 발견일로부터 180일 이내에 완화된 저위험 취약성, e. 조직 e: 취약성 검사 프로세스 및 보안 통제 평가에서 얻은 정보를 [할당: 조직이 정의한 직원 또는 역할]과 공유하여 다른 정보 시스템의 유사한 취약성(예: 시스템적 약점 또는 결함)을 제거하는 데 도움을 줍니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5	조직: a. 정보 시스템 및 호스팅된 애플리케이션에 대한 취약성 스캔을 [할당: 조직이 정의한 빈도 및/또는 조직이 정의한 프로세스에 따라 무작위로] 및 시스템/애플리케이션에 영향을 미칠 수 있는 새로운 취약성이 식별되고 보고되는 시점에 수행합니다. 조직 b: 다음에 대한 표준을 사용하여 도구 간의 상호 운용성을 촉진하고 취약성 관리 프로세스의 일부를 자동화하는 취약성 스캔 도구 및 기법을 사용합니다. 1. 플랫폼, 소프트웨어 결함 및 부적절한 구성 열거 2. 체크리스트 및 테스트 절차 형식 지정 3. 취약성 영향 측정 조직 c: 취약성 검사 보고서 및 보안 통제 평가 결과를 분석합니다. 조직 d: 조직의 위험 평가에 따라 정상적인 취약성을 [할당: 조직이 정의한 대응 시간] 내에 교정합니다. 조직 e: 취약성 검사 프로세스 및 보안 통제 평가에서 얻	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	은 정보를 [할당: 조직이 정의한 직원 또는 역할]과 공유하여 다른 정보 시스템의 유사한 취약성(예: 시스템적 약점 또는 결함)을 제거하는 데 도움을 줍니다.		
SA-3(a)	조직: a. 정보 보안 고려 사항을 포함하는 [할당: 조직이 정의한 시스템 개발 수명 주기]를 사용하여 정보 시스템을 관리합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-3(a)	조직: a. 정보 보안 고려 사항을 포함하는 [할당: 조직이 정의한 시스템 개발 수명 주기]를 사용하여 정보 시스템을 관리합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
SA-3(a)	조직: a. 정보 보안 고려 사항을 포함하는 [할당: 조직이 정의한 시스템 개발 수명 주기]를 사용하여 정보 시스템을 관리합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. 시스템, 구성 요소 또는 서비스 개발, 구현 및 운영 중에 구성 관리를 수행합니다. b. b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. 시스템, 구성 요소 또는 서비스 개발, 구현 및 운영 중에 구성 관리를 수행합니다. b. b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. 시스템, 구성 요소 또는 서비스 개발, 구현 및 운영 중에 구성 관리를 수행합니다. b. b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. 시스템, 구성 요소 또는 서비스 개발, 구현 및 운영 중에 구성 관리를 수행합니다. b. b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기 및 쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(5)	관리형 인터페이스의 정보 시스템은 기본적으로 네트워크 통신 트래픽을 거부하고 예외적으로 네트워크 통신 트래픽을 허용합니다(즉, 모두 거부, 예외에 의한 허용). 추가 지침: 이 제어 개선 사항은 인바운드 및 아웃바운드 네트워크 통신 트래픽에 모두 적용됩니다. deny-all, permit-by-exception 네트워크 통신 트래픽 정책은 필수적이고 승인된 연결만 허용하도록 보장합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-12	조직은 [할당: 키 생성, 배포, 저장, 액세스 및 폐기에 대한 조직이 정의한 요구 사항]에 따라 정보 시스템 내에서 사용되는 필수 암호화를 위한 암호화 키를 설정하고 관리합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-12	조직은 [할당: 키 생성, 배포, 저장, 액세스 및 폐기에 대한 조직이 정의한 요구 사항]에 따라 정보 시스템 내에서 사용되는 필수 암호화를 위한 암호화 키를 설정하고 관리합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
SC-12	조직은 [할당: 키 생성, 배포, 저장, 액세스 및 폐기에 대한 조직이 정의한 요구 사항]에 따라 정보 시스템 내에서 사용되는 필수 암호화를 위한 암호화 키를 설정하고 관리합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SI-2(2)	조직은 자동화된 메커니즘을 최소 매월 사용하여 결함 수정과 관련된 정보 시스템 구성 요소의 상태를 결정합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(2)	조직은 자동화된 메커니즘을 최소 매월 사용하여 결함 수정과 관련된 정보 시스템 구성 요소의 상태를 결정합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
SI-2(2)	조직은 자동화된 메커니즘을 최소 매월 사용하여 결함 수정과 관련된 정보 시스템 구성 요소의 상태를 결정합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(2)	조직은 자동화된 메커니즘을 최소 매월 사용하여 결함 수정과 관련된 정보 시스템 구성 요소의 상태를 결정합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3	조직: a. 정보 시스템 진입 및 출구 지점에 악성 코드 차단 메커니즘을 사용하여 악성 코드를 탐지하고 근절합니다. b. 조직 구성 관리 정책 및 절차에 따라 새 릴리스가 출시될 때마다 악성 코드 차단 메커니즘을 업데이트합니다. c. 악성 코드 차단 메커니즘을 다음과 같이 구성합니다. 1. 조직 보안 정책에 따라 파일을 다운로드, 열거나 실행할 때 정보 시스템을 [할당: 조직에서 정의한 빈도]로 정기적으로 검사하고 [선택 (하나 이상), 엔드포인트, 네트워크 진입/종료 지점]에서 외부 소스의 파일을 실시간으로 검사합니다. 2. [선택 (하나 이상): 악성 코드 차단, 악성 코드 격리, 관리자에게 알림 전송, [할당: 조직이 정의한 조치]] 악성 코드 탐지 대응, d. 악성 코드 탐지 및 제거 중에 오탐이 발생하여 정보 시스템의 가용성에 미칠 수 있는 잠재	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	적 영향을 해결합니다. 추가 지침: 정보 시스템 진입 및 출구 지점에는 방화벽, 전자 메일 서버, 웹 서버, 프록시 서버, 원격 액세스 서버, 워크스테이션, 노트북 컴퓨터, 모바일 디바이스 등이 포함됩니다. 악성 코드에는 바이러스, 웜, 트로이 목마, 스파이웨어 등이 포함됩니다. 악성 코드는 다양한 형식(예: UUENCODE, Unicode)으로 인코딩되거나, 압축 또는 숨겨진 파일 내에 포함되거나, 스테가노그래피를 사용하여 파일에 숨겨질 수도 있습니다. 악성 코드는 웹 액세스, 전자 메일, 전자 메일 첨부 파일, 휴대용 저장 장치 등 다양한 수단을 통해 전송될 수 있습니다. 악성 코드 삽입은 정보 시스템 취약성을 악용하여 발생합니다. 악성 코드 차단 메커니즘에는 바이러스 백신 시그니처 정의 및 평판 기반 기술 등이 포함됩니다. 악성 코드의 영향을 제한하		

제어 ID	제어 설명	AWS 구성 규칙	지침
	거나 제거하기 위한 다양한 기술과 방법이 있습니다. 광범위한 구성 관리 및 포괄적인 소프트웨어 무결성 제어는 무단 코드의 실행을 방지하는 데 효과적일 수 있습니다. 상용 소프트웨어 외에도 맞춤형 소프트웨어에도 악성 코드가 존재할 수 있습니다. 여기에는 로직 폭탄, 백도어 및 조직의 임무/비즈니스 기능에 영향을 미칠 수 있는 기타 유형의 사이버 공격 등이 포함될 수 있습니다. 기존의 악성 코드 차단 메커니즘이 이러한 코드를 항상 탐지할 수는 없습니다. 이러한 상황에서 조직은 소프트웨어가 의도한 기능 이외의 기능을 수행하지 않도록 하기 위한 보안 코딩 관행, 구성 관리 및 제어, 신뢰할 수 있는 조달 프로세스, 모니터링 관행 등 다른 보호 조치를 대신 사용합니다. 조직은 악성 코드 탐지에 대한 대응으로 다른 조치가 필요하다고 판단할 수 있습니다. 예		

제어 ID	제어 설명	AWS 구성 규칙	지침
	를 들어 조직에서는 정기 검사 중 악성 코드 탐지에 대한 대응 조치, 악성 다운로드 탐지에 대한 대응 조치 및/또는 파일을 열거나 실행하려 할 때의 악의성 탐지에 대한 대응 조치를 정의할 수 있습니다. 관련 규제 항목: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7 참고 문헌: NIST 특별 간행물 800-83.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3	조직: a. 정보 시스템 진입 및 출구 지점에 악성 코드 차단 메커니즘을 사용하여 악성 코드를 탐지하고 근절합니다. b. 조직 구성 관리 정책 및 절차에 따라 새 릴리스가 출시될 때마다 악성 코드 차단 메커니즘을 업데이트합니다. c. 악성 코드 차단 메커니즘을 다음과 같이 구성합니다. 1. 조직 보안 정책에 따라 파일을 다운로드, 열거나 실행할 때 정보 시스템을 [할당: 조직에서 정의한 빈도]로 정기적으로 검사하고 [선택 (하나 이상), 엔드포인트, 네트워크 진입/종료 지점]에서 외부 소스의 파일을 실시간으로 검사합니다. 2. [선택 (하나 이상): 악성 코드 차단, 악성 코드 격리, 관리자에게 알림 전송, [할당: 조직이 정의한 조치]] 악성 코드 탐지 대응, d. 악성 코드 탐지 및 제거 중에 오탐이 발생하여 정보 시스템의 가용성에 미칠 수 있는 잠재	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	적 영향을 해결합니다. 추가 지침: 정보 시스템 진입 및 출구 지점에는 방화벽, 전자 메일 서버, 웹 서버, 프록시 서버, 원격 액세스 서버, 워크스테이션, 노트북 컴퓨터, 모바일 디바이스 등이 포함됩니다. 악성 코드에는 바이러스, 웜, 트로이 목마, 스파이웨어 등이 포함됩니다. 악성 코드는 다양한 형식(예: UUENCODE, Unicode)으로 인코딩되거나, 압축 또는 숨겨진 파일 내에 포함되거나, 스테가노그래피를 사용하여 파일에 숨겨질 수도 있습니다. 악성 코드는 웹 액세스, 전자 메일, 전자 메일 첨부 파일, 휴대용 저장 장치 등 다양한 수단을 통해 전송될 수 있습니다. 악성 코드 삽입은 정보 시스템 취약성을 악용하여 발생합니다. 악성 코드 차단 메커니즘에는 바이러스 백신 시그니처 정의 및 평판 기반 기술 등이 포함됩니다. 악성 코드의 영향을 제한하		

제어 ID	제어 설명	AWS 구성 규칙	지침
	거나 제거하기 위한 다양한 기술과 방법이 있습니다. 광범위한 구성 관리 및 포괄적인 소프트웨어 무결성 제어는 무단 코드의 실행을 방지하는 데 효과적일 수 있습니다. 상용 소프트웨어 외에도 맞춤형 소프트웨어에도 악성 코드가 존재할 수 있습니다. 여기에는 로직 폭탄, 백도어 및 조직의 임무/비즈니스 기능에 영향을 미칠 수 있는 기타 유형의 사이버 공격 등이 포함될 수 있습니다. 기존의 악성 코드 차단 메커니즘이 이러한 코드를 항상 탐지할 수는 없습니다. 이러한 상황에서 조직은 소프트웨어가 의도한 기능 이외의 기능을 수행하지 않도록 하기 위한 보안 코딩 관행, 구성 관리 및 제어, 신뢰할 수 있는 조달 프로세스, 모니터링 관행 등 다른 보호 조치를 대신 사용합니다. 조직은 악성 코드 탐지에 대한 대응으로 다른 조치가 필요하다고 판단할 수 있습니다. 예		

제어 ID	제어 설명	AWS 구성 규칙	지침
	를 들어 조직에서는 정기 검사 중 악성 코드 탐지에 대한 대응 조치, 악성 다운로드 탐지에 대한 대응 조치 및/또는 파일을 열거나 실행하려 할 때의 악의성 탐지에 대한 대응 조치를 정의할 수 있습니다. 관련 규제 항목: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7 참고 문헌: NIST 특별 간행물 800-83.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3	조직: a. 정보 시스템 진입 및 출구 지점에 악성 코드 차단 메커니즘을 사용하여 악성 코드를 탐지하고 근절합니다. b. 조직 구성 관리 정책 및 절차에 따라 새 릴리스가 출시될 때마다 악성 코드 차단 메커니즘을 업데이트합니다. c. 악성 코드 차단 메커니즘을 다음과 같이 구성합니다. 1. 조직 보안 정책에 따라 파일을 다운로드, 열거나 실행할 때 정보 시스템을 [할당: 조직에서 정의한 빈도]로 정기적으로 검사하고 [선택 (하나 이상), 엔드포인트, 네트워크 진입/종료 지점]에서 외부 소스의 파일을 실시간으로 검사합니다. 2. [선택 (하나 이상): 악성 코드 차단, 악성 코드 격리, 관리자에게 알림 전송, [할당: 조직이 정의한 조치]] 악성 코드 탐지 대응, d. 악성 코드 탐지 및 제거 중에 오탐이 발생하여 정보 시스템의 가용성에 미칠 수 있는 잠재	ecs-task-definition-memory-hard-limit	Amazon Elastic Container Service(ECS) 컨테이너에 사용할 수 있는 최대 메모리를 제한하면 컨테이너에 악의적으로 액세스하는 경우 리소스 사용이 남용되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	적 영향을 해결합니다. 추가 지침: 정보 시스템 진입 및 출구 지점에는 방화벽, 전자 메일 서버, 웹 서버, 프록시 서버, 원격 액세스 서버, 워크스테이션, 노트북 컴퓨터, 모바일 디바이스 등이 포함됩니다. 악성 코드에는 바이러스, 웜, 트로이 목마, 스파이웨어 등이 포함됩니다. 악성 코드는 다양한 형식(예: UUENCODE, Unicode)으로 인코딩되거나, 압축 또는 숨겨진 파일 내에 포함되거나, 스테가노그래피를 사용하여 파일에 숨겨질 수도 있습니다. 악성 코드는 웹 액세스, 전자 메일, 전자 메일 첨부 파일, 휴대용 저장 장치 등 다양한 수단을 통해 전송될 수 있습니다. 악성 코드 삽입은 정보 시스템 취약성을 악용하여 발생합니다. 악성 코드 차단 메커니즘에는 바이러스 백신 시그니처 정의 및 평판 기반 기술 등이 포함됩니다. 악성 코드의 영향을 제한하		

제어 ID	제어 설명	AWS 구성 규칙	지침
	거나 제거하기 위한 다양한 기술과 방법이 있습니다. 광범위한 구성 관리 및 포괄적인 소프트웨어 무결성 제어는 무단 코드의 실행을 방지하는 데 효과적일 수 있습니다. 상용 소프트웨어 외에도 맞춤형 소프트웨어에도 악성 코드가 존재할 수 있습니다. 여기에는 로직 폭탄, 백도어 및 조직의 임무/비즈니스 기능에 영향을 미칠 수 있는 기타 유형의 사이버 공격 등이 포함될 수 있습니다. 기존의 악성 코드 차단 메커니즘이 이러한 코드를 항상 탐지할 수는 없습니다. 이러한 상황에서 조직은 소프트웨어가 의도한 기능 이외의 기능을 수행하지 않도록 하기 위한 보안 코딩 관행, 구성 관리 및 제어, 신뢰할 수 있는 조달 프로세스, 모니터링 관행 등 다른 보호 조치를 대신 사용합니다. 조직은 악성 코드 탐지에 대한 대응으로 다른 조치가 필요하다고 판단할 수 있습니다. 예		

제어 ID	제어 설명	AWS 구성 규칙	지침
	를 들어 조직에서는 정기 검사 중 악성 코드 탐지에 대한 대응 조치, 악성 다운로드 탐지에 대한 대응 조치 및/또는 파일을 열거나 실행하려 할 때의 악의성 탐지에 대한 대응 조치를 정의할 수 있습니다. 관련 규제 항목: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7 참고 문헌: NIST 특별 간행물 800-83.		
SI-4(1)	조직은 개별 침입 탐지 도구를 정보 시스템 전체의 침입 탐지 시스템에 연결하고 구성합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 지속적으로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 지속적으로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 지속적으로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 지속적으로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-5	조직: a. [할당: 조직에서 정의한 외부 조직]으로부터 정보 시스템 보안 경고, 권고 및 지침을 지속적으로 받습니다. b. 필요하다고 판단되는 경우 내부 보안 경고, 권고 및 지침을 생성합니다. c. 보안 경고, 권고 및 지침을 다음에 전파합니다. [선택 (한나 이상): [할당: 조직에서 정의한 직원 또는 역할], [할당: 조직에서 정의한 조직 내 요소], [할당: 조직에서 정의한 외부 조직]] d. 정해진 일정에 따라 보안 지침을 구현하거나 발급 조직에 미준수 정도를 알립니다. 추가 지침: 미국 컴퓨터 비상 준비 팀(US-CERT)은 연방 정부 전체에 상황 인식을 유지하기 위해 보안 경고 및 권고를 생성합니다. 보안 지침은 OMB 또는 해당 지침을 발행할 책임과 권한을 가진 기타 지정 기관에서 발행합니다. 이러한 지침 중 상당수가 매우 중요하며, 지침이 적시에 시	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	행되지 않을 경우 조직 운영 및 자산, 개인, 기타 조직 및 국가에 즉각적인 악영향을 미칠 수 있기 때문에 보안 지침을 준수하는 것이 필수적입니다. 외부 조직에는 예를 들어 외부 미션/비즈니스 파트너, 공급망 파트너, 외부 서비스 제공업체 및 기타 동료/지원 조직이 포함됩니다. 관련 통제: SI-2. 참고 문헌: NIST 특별 간행물 800-40.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-5	조직: a. [할당: 조직에서 정의한 외부 조직]으로부터 정보 시스템 보안 경고, 권고 및 지침을 지속적으로 받습니다. b. 필요하다고 판단되는 경우 내부 보안 경고, 권고 및 지침을 생성합니다. c. 보안 경고, 권고 및 지침을 다음에 전파합니다. [선택 (한나 이상): [할당: 조직에서 정의한 직원 또는 역할], [할당: 조직에서 정의한 조직 내 요소], [할당: 조직에서 정의한 외부 조직]] d. 정해진 일정에 따라 보안 지침을 구현하거나 발급 조직에 미준수 정도를 알립니다. 추가 지침: 미국 컴퓨터 비상 준비 팀(US-CERT)은 연방 정부 전체에 상황 인식을 유지하기 위해 보안 경고 및 권고를 생성합니다. 보안 지침은 OMB 또는 해당 지침을 발행할 책임과 권한을 가진 기타 지정 기관에서 발행합니다. 이러한 지침 중 상당수가 매우 중요하며, 지침이 적시에 시	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	행되지 않을 경우 조직 운영 및 자산, 개인, 기타 조직 및 국가에 즉각적인 악영향을 미칠 수 있기 때문에 보안 지침을 준수하는 것이 필수적입니다. 외부 조직에는 예를 들어 외부 미션/비즈니스 파트너, 공급망 파트너, 외부 서비스 제공업체 및 기타 동료/지원 조직이 포함됩니다. 관련 통제: SI-2. 참고 문헌: NIST 특별 간행물 800-40.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-5	조직: a. [할당: 조직에서 정의한 외부 조직]으로부터 정보 시스템 보안 경고, 권고 및 지침을 지속적으로 받습니다. b. 필요하다고 판단되는 경우 내부 보안 경고, 권고 및 지침을 생성합니다. c. 보안 경고, 권고 및 지침을 다음에 전파합니다. [선택 (한나 이상): [할당: 조직에서 정의한 직원 또는 역할], [할당: 조직에서 정의한 조직 내 요소], [할당: 조직에서 정의한 외부 조직]] d. 정해진 일정에 따라 보안 지침을 구현하거나 발급 조직에 미준수 정도를 알립니다. 추가 지침: 미국 컴퓨터 비상 준비 팀(US-CERT)은 연방 정부 전체에 상황 인식을 유지하기 위해 보안 경고 및 권고를 생성합니다. 보안 지침은 OMB 또는 해당 지침을 발행할 책임과 권한을 가진 기타 지정 기관에서 발행합니다. 이러한 지침 중 상당수가 매우 중요하며, 지침이 적시에 시	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	행되지 않을 경우 조직 운영 및 자산, 개인, 기타 조직 및 국가에 즉각적인 악영향을 미칠 수 있기 때문에 보안 지침을 준수하는 것이 필수적입니다. 외부 조직에는 예를 들어 외부 미션/비즈니스 파트너, 공급망 파트너, 외부 서비스 제공업체 및 기타 동료/지원 조직이 포함됩니다. 관련 통제: SI-2. 참고 문헌: NIST 특별 간행물 800-40.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-5	조직: a. [할당: 조직에서 정의한 외부 조직]으로부터 정보 시스템 보안 경고, 권고 및 지침을 지속적으로 받습니다. b. 필요하다고 판단되는 경우 내부 보안 경고, 권고 및 지침을 생성합니다. c. 보안 경고, 권고 및 지침을 다음에 전파합니다. [선택 (한나 이상): [할당: 조직에서 정의한 직원 또는 역할], [할당: 조직에서 정의한 조직 내 요소], [할당: 조직에서 정의한 외부 조직]] d. 정해진 일정에 따라 보안 지침을 구현하거나 발급 조직에 미준수 정도를 알립니다. 추가 지침: 미국 컴퓨터 비상 준비 팀(US-CERT)은 연방 정부 전체에 상황 인식을 유지하기 위해 보안 경고 및 권고를 생성합니다. 보안 지침은 OMB 또는 해당 지침을 발행할 책임과 권한을 가진 기타 지정 기관에서 발행합니다. 이러한 지침 중 상당수가 매우 중요하며, 지침이 적시에 시	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	행되지 않을 경우 조직 운영 및 자산, 개인, 기타 조직 및 국가에 즉각적인 악영향을 미칠 수 있기 때문에 보안 지침을 준수하는 것이 필수적입니다. 외부 조직에는 예를 들어 외부 미션/비즈니스 파트너, 공급망 파트너, 외부 서비스 제공업체 및 기타 동료/지원 조직이 포함됩니다. 관련 통제: SI-2. 참고 문헌: NIST 특별 간행물 800-40.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(1)	정보 시스템은 적어도 한 달에 한 번 무결성 검사 보안 관련 이벤트를 수행합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(1)	정보 시스템은 적어도 한 달에 한 번 무결성 검사 보안 관련 이벤트를 수행합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
SI-7(1)	정보 시스템은 적어도 한 달에 한 번 무결성 검사 보안 관련 이벤트를 수행합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7	조직은 무결성 검증 도구를 사용하여 [할당: 조직 정의 소프트웨어, 펌웨어 및 정보]의 무단 변경을 탐지합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	[api-gw-execution-logging-enabled](#)	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-16	정보 시스템은 무단 코드 실행으로부터 메모리를 보호하기 위해 [할당: 조직에서 정의한 보안 보호 장치]를 구현합니다. 추가 지침: 일부 공격자는 실행 불가능한 메모리 영역이나 금지된 메모리 위치에서 코드를 실행하려는 의도로 공격을 시작합니다. 메모리 보호를 위해 사용되는 보안 보호 장치에는 데이터 실행 방지 및 주소 공간 레이아웃 무작위화 등이 포함됩니다. 데이터 실행 방지 보호 장치는 하드웨어에 적용하거나 메커니즘의 강도를 높이는 하드웨어와 함께 소프트웨어에 적용할 수 있습니다. 관련 규제 항목: AC-25, SC-3. 제어 개선 사항: 없음. 참고: 없음.	ecs-task-definition-memory-hard-limit	Amazon Elastic Container Service(ECS) 컨테이너에 사용할 수 있는 최대 메모리를 제한하면 컨테이너에 악의적으로 액세스하는 경우 리소스 사용이 남용되는 것을 방지할 수 있습니다.

템플릿

템플릿은 GitHub: FedRAMP(Moderate) 운영 모범 사례에서 확인할 수 있습니다.

FedRAMP(High 파트 1) 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Federal Risk and Authorization Management Program(FedRAMP)과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 FedRAMP 제어와 관련이 있습니다. FedRAMP 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	elb-acm-certificate-required	다음 내용을 채웁니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	access-keys-rotated	조직 정책에 따라 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정을 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(12)(a)	조직: a. 정보 시스템 계정의 [할당: 조직에서 정의한 비정형 용도] 활동을 모니터링합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(12)(a)	조직: a. 정보 시스템 계정의 [할당: 조직에서 정의한 비정형 용도] 활동을 모니터링합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(3)	정보 시스템은 90일이 지나면 사용자 계정의 비활성 계정을 자동으로 비활성화합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(3)	정보 시스템은 90일이 지나면 사용자 계정의 비활성 계정을 자동으로 비활성화합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정을 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	access-keys-rotated	조직 정책에 따라 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	access-keys-rotated	조직 정책에 따라 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정을 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 IAM 사용자가 하나 이상 있도록 하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 IAM 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 방법이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정을 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)를 사용하면 IAM 그룹에 IAM 사용자가 하나 이상 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합할 수 있습니다. 관련 권한 또는 직무에 따라 IAM 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 방법이 될 수 있습니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)를 사용하면 IAM 그룹에 IAM 사용자가 하나 이상 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합할 수 있습니다. 관련 권한 또는 직무에 따라 IAM 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 방법이 될 수 있습니다.
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정을 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)를 사용하면 IAM 그룹에 IAM 사용자가 하나 이상 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합할 수 있습니다. 관련 권한 또는 직무에 따라 IAM 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 방법이 될 수 있습니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정을 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(2)	정보 시스템은 비보안 함수에 액세스할 때 권한 없는 계정을 사용해야 하므로 권한 있는 계정 또는 역할 내에서 작동할 때 노출을 제한합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-6(2)	정보 시스템은 비보안 함수에 액세스할 때 권한 없는 계정을 사용해야 하므로 권한 있는 계정 또는 역할 내에서 작동할 때 노출을 제한합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(2)	정보 시스템은 비보안 함수에 액세스할 때 권한 없는 계정을 사용해야 하므로 권한 있는 계정 또는 역할 내에서 작동할 때 노출을 제한합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정을 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
AC-6(9)	정보 시스템이 권한 있는 함수의 실행을 기록합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	정보 시스템이 권한 있는 함수의 실행을 기록합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	정보 시스템이 권한 있는 함수의 실행을 기록합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	정보 시스템이 권한 있는 함수의 실행을 기록합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AC-6(9)	정보 시스템이 권한 있는 함수의 실행을 기록합니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	정보 시스템이 권한 있는 함수의 실행을 기록합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	정보 시스템이 권한 있는 함수의 실행을 기록합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	정보 시스템이 권한 있는 함수의 실행을 기록합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(10)	정보 시스템은 권한이 없는 사용자가 구현된 보안 보호 장치 및 대응 조치를 비활성화, 우회 또는 변경하는 것을 포함하는 권한 있는 기능을 실행하는 것을 방지합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정을 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
AC-6(10)	정보 시스템은 권한이 없는 사용자가 구현된 보안 보호 장치 및 대응 조치를 비활성화, 우회 또는 변경하는 것을 포함하는 권한 있는 기능을 실행하는 것을 방지합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(10)	정보 시스템은 권한이 없는 사용자가 구현된 보안 보호 장치 및 대응 조치를 비활성화, 우회 또는 변경하는 것을 포함하는 권한 있는 기능을 실행하는 것을 방지합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AU-11	조직은 보안 사고에 대한 사후 조사를 지원하고 규정 및 조직의 정보 보존 요구 사항을 충족하기 위해 최소 90일 동안 감사 기록을 보관합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-6(3)	조직이 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-7	정보 시스템이 감사 레코드 감소와 보고서 생성 기능을 제공하고 구현합니다. a. 온디맨드 감사 레코드 검토, 분석 및 보고 요구 사항과 사고에 대한 사후 조사를 지원합니다. b. 감사 레코드의 원본 콘텐츠 또는 시간 순서를 변경하지 않습니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.
AU-7	정보 시스템이 감사 레코드 감소와 보고서 생성 기능을 제공하고 구현합니다. a. 온디맨드 감사 레코드 검토, 분석 및 보고 요구 사항과 사고에 대한 사후 조사를 지원합니다. b. 감사 레코드의 원본 콘텐츠 또는 시간 순서를 변경하지 않습니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-7(1)	정보 시스템은 [할당: 감사 기록 내 조직이 정의한 감사 필드]를 기반으로 관심 이벤트에 대한 감사 기록을 처리할 수 있는 기능을 제공합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
AU-7(1)	정보 시스템은 [할당: 감사 기록 내 조직이 정의한 감사 필드]를 기반으로 관심 이벤트에 대한 감사 기록을 처리할 수 있는 기능을 제공합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9	정보 시스템은 감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
AU-9	정보 시스템은 감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
AU-9	정보 시스템은 감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9(2)	정보 시스템은 감사 기록을 최소한 매주 감사 대상 시스템 또는 구성 요소와 물리적으로 다른 시스템 또는 시스템 구성 요소에 백업합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
AU-9(2)	정보 시스템은 감사 기록을 최소한 매주 감사 대상 시스템 또는 구성 요소와 물리적으로 다른 시스템 또는 시스템 구성 요소에 백업합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	정보 시스템이 [할당: 조직 정의 시스템 구성 요소]의 AU-2a에 정의된 대로 시스템이 감사할 수 있는 이벤트 유형에 대한 감사 레코드 생성 기능을 제공합니다. b. [할당: 조직에서 정의한 직원 또는 역할]이 시스템의 특정 구성 요소에 의해 로깅될 이벤트 유형을 선택할 수 있도록 허용합니다. c. AU-3에 정의된 감사 레코드 콘텐츠를 포함하는 AU-2c에 정의된 이벤트 유형에 대한 감사 레코드를 생성합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 강화된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-7(a)	조직: a. 필수 기능만 제공하도록 정보 시스템을 구성합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-7(a)	조직: a. 필수 기능만 제공하도록 정보 시스템을 구성합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
CM-7(a)	조직: a. 필수 기능만 제공하도록 정보 시스템을 구성합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(1)	조직은 구성 요소 설치, 제거 및 정보 시스템 업데이트의 필수 부분으로 정보 시스템 구성 요소 인벤토리를 업데이트합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(1)	조직은 구성 요소 설치, 제거 및 정보 시스템 업데이트의 필수 부분으로 정보 시스템 구성 요소 인벤토리를 업데이트합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(3)(a)	조직: a. 탐지 시 최대 5분 지연되는 자동 메커니즘을 사용하여 정보 시스템 내에 승인되지 않은 하드웨어, 소프트웨어 및 펌웨어 구성 요소가 있는지 탐지하는 자동 메커니즘을 지속적으로 적용합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(3)(a)	조직: a. 탐지 시 최대 5분 지연되는 자동 메커니즘을 사용하여 정보 시스템 내에 승인되지 않은 하드웨어, 소프트웨어 및 펌웨어 구성 요소가 있는지 탐지하는 자동 메커니즘을 지속적으로 적용합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
CM-8(3)(a)	조직: a. 탐지 시 최대 5분 지연되는 자동 메커니즘을 사용하여 정보 시스템 내에 승인되지 않은 하드웨어, 소프트웨어 및 펌웨어 구성 요소가 있는지 탐지하는 자동 메커니즘을 지속적으로 적용합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(3)(a)	조직: a. 탐지 시 최대 5분 지연되는 자동 메커니즘을 사용하여 정보 시스템 내에 승인되지 않은 하드웨어, 소프트웨어 및 펌웨어 구성 요소가 있는지 탐지하는 자동 메커니즘을 지속적으로 적용합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CP-6 (1)	동일한 위협에 대한 취약성을 줄이기 위해 조직이 기본 스토리지 사이트와 충분히 분리된 대체 스토리지 사이트를 식별합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6 (1)	동일한 위협에 대한 취약성을 줄이기 위해 조직이 기본 스토리지 사이트와 충분히 분리된 대체 스토리지 사이트를 식별합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-6 (1)	동일한 위협에 대한 취약성을 줄이기 위해 조직이 기본 스토리지 사이트와 충분히 분리된 대체 스토리지 사이트를 식별합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6 (1)	동일한 위협에 대한 취약성을 줄이기 위해 조직이 기본 스토리지 사이트와 충분히 분리된 대체 스토리지 사이트를 식별합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
CP-6 (1)	동일한 위협에 대한 취약성을 줄이기 위해 조직이 기본 스토리지 사이트와 충분히 분리된 대체 스토리지 사이트를 식별합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6 (1)	동일한 위협에 대한 취약성을 줄이기 위해 조직이 기본 스토리지 사이트와 충분히 분리된 대체 스토리지 사이트를 식별합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CP-6 (1)	동일한 위협에 대한 취약성을 줄이기 위해 조직이 기본 스토리지 사이트와 충분히 분리된 대체 스토리지 사이트를 식별합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6 (1)	동일한 위협에 대한 취약성을 줄이기 위해 조직이 기본 스토리지 사이트와 충분히 분리된 대체 스토리지 사이트를 식별합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	redshift-cluster-maintenancesettings-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	정보 시스템: a. [할당: 조직 정의 시스템 구성 요소] [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]에 포함된 사용자 수준 정보의 백업을 수행합니다. b. 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다. c. 보안 및 개인정보 보호 관련 문서 [할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 빈도]를 포함한 시스템 문서의 백업을 수행합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보를 백업합니다(매일 증분, 매주 전체).	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2	정보 시스템은 조직 사용자(또는 조직 사용자를 대신하여 활동하는 프로세스)를 고유하게 식별하고 인증합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IA-2	정보 시스템은 조직 사용자(또는 조직 사용자를 대신하여 활동하는 프로세스)를 고유하게 식별하고 인증합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정을 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
IA-2(1)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(1)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(1)(2)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다. (2) 정보 시스템은 권한이 없는 계정에 대한 네트워크 액세스를 위해 다중 인증을 구현합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
IA-2(1)(2)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다. (2) 정보 시스템은 권한이 없는 계정에 대한 네트워크 액세스를 위해 다중 인증을 구현합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-5(1)(a)(d)(e)	암호 기반 인증을 위한 정보 시스템: a. a. 최소한의 암호 복잡성 수준 강제[할당: 각 유형에 대한 최소 요구 사항을 포함하여 대소문자 구분, 문자 수, 대소문자 혼합, 숫자 및 특수 문자에 대한 조직에서 정의한 요구 사항] d. 암호의 최소 및 최대 수명 제한 적용[할당: 조직에서 정의한 최소 수명 및 최대 수명] 24회 생성에 암호 재사용을 금지합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-5(4)	조직에서는 자동화된 도구를 사용하여 암호 인증자가 [할당: 조직에서 정의한 요구 사항]을 충족할 만큼 충분히 강력한지 판단합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IA-5(7)	조직은 암호화되지 않은 정적 인증자가 애플리케이션이나 액세스 스크립트에 내장되거나 기능 키에 저장되지 않도록 합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-6(1)	조직은 자동화된 메커니즘을 사용하여 보안 인시던트를 보고하는 것을 지원합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
IR-6(1)	조직은 자동화된 메커니즘을 사용하여 보안 인시던트를 보고하는 것을 지원합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-6(1)	조직은 자동화된 메커니즘을 사용하여 보안 인시던트를 보고하는 것을 지원합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-7(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 대응 관련 정보 및 지원의 가용성을 높입니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
IR-7(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 대응 관련 정보 및 지원의 가용성을 높입니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-7(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 대응 관련 정보 및 지원의 가용성을 높입니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5	조직: a. 정보 시스템 및 호스팅된 애플리케이션에 대한 취약성 스캔을 [할당: 조직이 정의한 빈도 및/또는 조직이 정의한 프로세스에 따라 무작위로] 및 시스템/애플리케이션에 영향을 미칠 수 있는 새로운 취약성이 식별되고 보고되는 시점에 수행합니다. 조직 b: 다음에 대한 표준을 사용하여 도구 간의 상호 운용성을 촉진하고 취약성 관리 프로세스의 일부를 자동화하는 취약성 스캔 도구 및 기법을 사용합니다. 1. 플랫폼, 소프트웨어 결함 및 부적절한 구성 열거 2. 체크리스트 및 테스트 절차 형식 지정 3. 취약성 영향 측정 조직 c: 취약성 검사 보고서 및 보안 통제 평가 결과를 분석합니다. 조직 d: 조직의 위험 평가에 따라 정상적인 취약성을 [할당: 조직이 정의한 대응 시간] 내에 교정합니다. 조직 e: 취약성 검사 프로세스 및 보안 통제 평가에서 얻	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	은 정보를 [할당: 조직이 정의한 직원 또는 역할]과 공유하여 다른 정보 시스템의 유사한 취약성(예: 시스템적 약점 또는 결함)을 제거하는 데 도움을 줍니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5	조직: a. 매월 [운영 체제/인프라, 월간 웹 애플리케이션 및 데이터베이스], 그리고 시스템/애플리케이션에 영향을 미칠 수 있는 새로운 취약성이 식별되고 보고되는 시점을 기준으로 정보 시스템 및 호스팅된 애플리케이션의 취약성을 검사합니다. b. 조직 b: 다음에 대한 표준을 사용하여 도구 간의 상호 운용성을 촉진하고 취약성 관리 프로세스의 일부를 자동화하는 취약성 스캔 도구 및 기법을 사용합니다. 1. 플랫폼, 소프트웨어 결함 및 부적절한 구성 열거 2. 체크리스트 및 테스트 절차 형식 지정 3. 취약성 영향 측정 조직 c: 취약성 검사 보고서 및 보안 통제 평가 결과를 분석합니다. 합법적인 취약성을 해결합니다. 조직의 위험 평가에 따라 발견일로부터 30일 이내에 완화된 고위험 취약성, 발견일로부터 90일 이내에 완화된 중간 위험 취약	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	성, 발견일로부터 180일 이내에 완화된 저위험 취약성, e. 조직 e: 취약성 검사 프로세스 및 보안 통제 평가에서 얻은 정보를 [할당: 조직이 정의한 직원 또는 역할]과 공유하여 다른 정보 시스템의 유사한 취약성(예: 시스템적 약점 또는 결함)을 제거하는 데 도움을 줍니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. 시스템, 구성 요소 또는 서비스 개발, 구현 및 운영 중에 구성 관리를 수행합니다. b. b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. 시스템, 구성 요소 또는 서비스 개발, 구현 및 운영 중에 구성 관리를 수행합니다. b. b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. 시스템, 구성 요소 또는 서비스 개발, 구현 및 운영 중에 구성 관리를 수행합니다. b. b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. 시스템, 구성 요소 또는 서비스 개발, 구현 및 운영 중에 구성 관리를 수행합니다. b. b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-3(a)	조직: a. 정보 보안 고려 사항을 포함하는 [할당: 조직이 정의한 시스템 개발 수명 주기]를 사용하여 정보 시스템을 관리합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-3(a)	조직: a. 정보 보안 고려 사항을 포함하는 [할당: 조직이 정의한 시스템 개발 수명 주기]를 사용하여 정보 시스템을 관리합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
SA-3(a)	조직: a. 정보 보안 고려 사항을 포함하는 [할당: 조직이 정의한 시스템 개발 수명 주기]를 사용하여 정보 시스템을 관리합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 사용자 이름 및 암호가 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰 또는 사용자 이름과 암호 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스하기 위한 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-12	조직은 [할당: 키 생성, 배포, 저장, 액세스 및 폐기에 대한 조직이 정의한 요구 사항]에 따라 정보 시스템 내에서 사용되는 필수 암호화를 위한 암호화 키를 설정하고 관리합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암 호화 기간이 종료되면 키가 교체되도록 합니다.
SC-12	조직은 [할당: 키 생성, 배포, 저장, 액세스 및 폐기에 대한 조직이 정의한 요구 사항]에 따라 정보 시스템 내에서 사용되는 필수 암호화를 위한 암호화 키를 설정하고 관리합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-12	조직은 [할당: 키 생성, 배포, 저장, 액세스 및 폐기에 대한 조직이 정의한 요구 사항]에 따라 정보 시스템 내에서 사용되는 필수 암호화를 위한 암호화 키를 설정하고 관리합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 IAM 사용자가 하나 이상 있도록 하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 IAM 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 방법이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 기밀성과 무결성을 보호합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스를 통한 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기 및 쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8	정보 시스템은 전송된 정보의 기밀성과 무결성을 보호합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-2(2)	조직은 자동화된 메커니즘을 최소 매월 사용하여 결함 수정과 관련된 정보 시스템 구성 요소의 상태를 결정합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(2)	조직은 자동화된 메커니즘을 최소 매월 사용하여 결함 수정과 관련된 정보 시스템 구성 요소의 상태를 결정합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(2)	조직은 자동화된 메커니즘을 최소 매월 사용하여 결함 수정과 관련된 정보 시스템 구성 요소의 상태를 결정합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
SI-2(2)	조직은 자동화된 메커니즘을 최소 매월 사용하여 결함 수정과 관련된 정보 시스템 구성 요소의 상태를 결정합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(1)	조직은 개별 침입 탐지 도구를 정보 시스템 전체의 침입 탐지 시스템에 연결하고 구성합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 지속적으로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 지속적으로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 지속적으로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 지속적으로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7	조직은 무결성 검증 도구를 사용하여 [할당: 조직 정의 소프트웨어, 펌웨어 및 정보]의 무단 변경을 탐지합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(1)	정보 시스템은 적어도 한 달에 한 번 무결성 검사 보안 관련 이벤트를 수행합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
SI-7(1)	정보 시스템은 적어도 한 달에 한 번 무결성 검사 보안 관련 이벤트를 수행합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(1)	정보 시스템은 적어도 한 달에 한 번 무결성 검사 보안 관련 이벤트를 수행합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5(1)	조직은 검사할 정보 시스템 취약성을 즉시 업데이트할 수 있는 기능이 포함된 취약성 검사 도구를 사용합니다. 보충 지침: 새로운 취약성이 발견되고 발표되고 검사 방법이 개발되면 검사할 취약성을 즉시 업데이트해야 합니다. 이 업데이트 프로세스는 정보 시스템의 잠재적 취약성을 최대한 빨리 식별하고 해결하는 데 도움이 됩니다. 관련 규제 항목: SI-3, SI-7.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5(1)	조직은 검사할 정보 시스템 취약성을 즉시 업데이트할 수 있는 기능이 포함된 취약성 검사 도구를 사용합니다. 보충 지침: 새로운 취약성이 발견되고 발표되고 검사 방법이 개발되면 검사할 취약성을 즉시 업데이트해야 합니다. 이 업데이트 프로세스는 정보 시스템의 잠재적 취약성을 최대한 빨리 식별하고 해결하는 데 도움이 됩니다. 관련 규제 항목: SI-3, SI-7.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-5(1)	조직은 검사할 정보 시스템 취약성을 즉시 업데이트할 수 있는 기능이 포함된 취약성 검사 도구를 사용합니다. 보충 지침: 새로운 취약성이 발견되고 발표되고 검사 방법이 개발되면 검사할 취약성을 즉시 업데이트해야 합니다. 이 업데이트 프로세스는 정보 시스템의 잠재적 취약성을 최대한 빨리 식별하고 해결하는 데 도움이 됩니다. 관련 규제 항목: SI-3, SI-7.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	조직: (a) 각 외부 통신 서비스에 대한 관리 인터페이스를 구현하고, (b) 각 관리 인터페이스에 대한 트래픽 흐름 정책을 수립하고, (c) 각 인터페이스를 통해 전송되는 정보의 기밀성과 무결성을 보호하고, (d) 트래픽 흐름 정책에 대한 각 예외를 지원하는 임무/비즈니스 요구 사항 및 해당 요구 기간과 함께 문서화하고, (e) 트래픽 흐름 정책에 대한 예외를 검토하고 [할당: 조직에서 정의한 빈도] 명시적 임무/비즈니스 필요에서 더 이상 지원되지 않는 예외를 제거합니다. 추가 지침: 관련 제어: SC-8.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(5)	관리형 인터페이스의 정보 시스템은 기본적으로 네트워크 통신 트래픽을 거부하고 예외적으로 네트워크 통신 트래픽을 허용합니다(즉, 모두 거부, 예외에 의한 허용). 추가 지침: 이 제어 개선 사항은 인바운드 및 아웃바운드 네트워크 통신 트래픽에 모두 적용됩니다. deny-all, permit-by-exception 네트워크 통신 트래픽 정책은 필수적이고 승인된 연결만 허용하도록 보장합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자 계정을 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자 계정을 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자 계정을 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자 계정을 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 IAM 사용자가 하나 이상 있도록 하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 IAM 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 방법이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자 계정을 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(7)	조직은 (a) 허용된 정보 시스템 액세스 및 권한을 역할별로 구성하는 역할 기반 액세스 체계에 따라 권한이 있는 사용자 계정을 설정하고 관리합니다. (b) 권한이 부여된 역할 할당을 모니터링합니다. (c) 권한이 부여된 역할 할당이 더 이상 적절하지 않을 경우 [할당: 조직에서 정의한 조치]를 수행합니다. 추가 지침: 권한이 있는 역할은 개인에게 할당되는 조직 정의 역할로, 이러한 개인은 일반 사용자가 수행할 수 없는 특정 보안 관련 기능을 수행할 수 있습니다. 이러한 권한 있는 역할에는 키 관리, 계정 관리, 네트워크 및 시스템 관리, 데이터베이스 관리, 웹 관리 등이 포함됩니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	[api-gw-execution-logging-enabled](#)	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-11	정보 시스템: a. 공격자가 악용할 수 있는 정보는 밝히지 않으면서 시정 조치에 필요한 정보를 제공하는 오류 메시지를 생성합니다. b. [할당: 조직에서 정의한 직원 또는 역할]에게만 오류 메시지를 표시합니다. 추가 지침: 조직에서는 오류 메시지의 구조/내용을 신중하게 고려합니다. 정보 시스템이 오류 조건을 식별하고 처리할 수 있는 정도는 조직 정책 및 운영 요구 사항에 따라 결정됩니다. 공격자가 악용할 수 있는 정보에는 예를 들어 사용자 이름으로 잘못 입력한 암호를 사용한 잘못된 로그온 시도, 기록된 정보에서 파생될 수 있는 (명시적으로 밝히지 않은 경우) 사명/비즈니스 정보, 계좌 번호, 주민등록번호, 신용 카드 번호와 같은 개인 정보가 있습니다. 또한 오류 메시지는 정보를 전송하기 위한 은밀한 채널을 제공할 수 있습니다. 관	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련 규제: AU-2, AU-3, SC-31. 제어 개선 사항: 없음. 참고: 없음.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3	조직: a. 정보 시스템 진입 및 출구 지점에 악성 코드 차단 메커니즘을 사용하여 악성 코드를 탐지하고 근절합니다. b. 조직 구성 관리 정책 및 절차에 따라 새 릴리스가 출시될 때마다 악성 코드 차단 메커니즘을 업데이트합니다. c. 악성 코드 차단 메커니즘을 다음과 같이 구성합니다. 1. 조직 보안 정책에 따라 파일을 다운로드, 열거나 실행할 때 정보 시스템을 [할당: 조직에서 정의한 빈도]로 정기적으로 검사하고 [선택 (하나 이상), 엔드포인트, 네트워크 진입/종료 지점]에서 외부 소스의 파일을 실시간으로 검사합니다. 2. [선택 (하나 이상): 악성 코드 차단, 악성 코드 격리, 관리자에게 알림 전송, [할당: 조직이 정의한 조치]] 악성 코드 탐지 대응, d. 악성 코드 탐지 및 제거 중에 오탐이 발생하여 정보 시스템의 가용성에 미칠 수 있는 잠재	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	적 영향을 해결합니다. 추가 지침: 정보 시스템 진입 및 출구 지점에는 방화벽, 전자 메일 서버, 웹 서버, 프록시 서버, 원격 액세스 서버, 워크스테이션, 노트북 컴퓨터, 모바일 디바이스 등이 포함됩니다. 악성 코드에는 바이러스, 웜, 트로이 목마, 스파이웨어 등이 포함됩니다. 악성 코드는 다양한 형식(예: UUENCODE, Unicode)으로 인코딩되거나, 압축 또는 숨겨진 파일 내에 포함되거나, 스테가노그래피를 사용하여 파일에 숨겨질 수도 있습니다. 악성 코드는 웹 액세스, 전자 메일, 전자 메일 첨부 파일, 휴대용 저장 장치 등 다양한 수단을 통해 전송될 수 있습니다. 악성 코드 삽입은 정보 시스템 취약성을 악용하여 발생합니다. 악성 코드 차단 메커니즘에는 바이러스 백신 시그니처 정의 및 평판 기반 기술 등이 포함됩니다. 악성 코드의 영향을 제한하		

제어 ID	제어 설명	AWS 구성 규칙	지침
	거나 제거하기 위한 다양한 기술과 방법이 있습니다. 광범위한 구성 관리 및 포괄적인 소프트웨어 무결성 제어는 무단 코드의 실행을 방지하는 데 효과적일 수 있습니다. 상용 소프트웨어 외에도 맞춤형 소프트웨어에도 악성 코드가 존재할 수 있습니다. 여기에는 로직 폭탄, 백도어 및 조직의 임무/비즈니스 기능에 영향을 미칠 수 있는 기타 유형의 사이버 공격 등이 포함될 수 있습니다. 기존의 악성 코드 차단 메커니즘이 이러한 코드를 항상 탐지할 수는 없습니다. 이러한 상황에서 조직은 소프트웨어가 의도한 기능 이외의 기능을 수행하지 않도록 하기 위한 보안 코딩 관행, 구성 관리 및 제어, 신뢰할 수 있는 조달 프로세스, 모니터링 관행 등 다른 보호 조치를 대신 사용합니다. 조직은 악성 코드 탐지에 대한 대응으로 다른 조치가 필요하다고 판단할 수 있습니다. 예		

제어 ID	제어 설명	AWS 구성 규칙	지침
	를 들어 조직에서는 정기 검사 중 악성 코드 탐지에 대한 대응 조치, 악성 다운로드 탐지에 대한 대응 조치 및/또는 파일을 열거나 실행하려 할 때의 악의성 탐지에 대한 대응 조치를 정의할 수 있습니다. 관련 규제 항목: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7 참고 문헌: NIST 특별 간행물 800-83.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3	조직: a. 정보 시스템 진입 및 출구 지점에 악성 코드 차단 메커니즘을 사용하여 악성 코드를 탐지하고 근절합니다. b. 조직 구성 관리 정책 및 절차에 따라 새 릴리스가 출시될 때마다 악성 코드 차단 메커니즘을 업데이트합니다. c. 악성 코드 차단 메커니즘을 다음과 같이 구성합니다. 1. 조직 보안 정책에 따라 파일을 다운로드, 열거나 실행할 때 정보 시스템을 [할당: 조직에서 정의한 빈도]로 정기적으로 검사하고 [선택 (하나 이상), 엔드포인트, 네트워크 진입/종료 지점]에서 외부 소스의 파일을 실시간으로 검사합니다. 2. [선택 (하나 이상): 악성 코드 차단, 악성 코드 격리, 관리자에게 알림 전송, [할당: 조직이 정의한 조치]] 악성 코드 탐지 대응, d. 악성 코드 탐지 및 제거 중에 오탐이 발생하여 정보 시스템의 가용성에 미칠 수 있는 잠재	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 사용자 이름 및 암호가 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰 또는 사용자 이름과 암호 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스하기 위한 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	적 영향을 해결합니다. 추가 지침: 정보 시스템 진입 및 출구 지점에는 방화벽, 전자 메일 서버, 웹 서버, 프록시 서버, 원격 액세스 서버, 워크스테이션, 노트북 컴퓨터, 모바일 디바이스 등이 포함됩니다. 악성 코드에는 바이러스, 웜, 트로이 목마, 스파이웨어 등이 포함됩니다. 악성 코드는 다양한 형식(예: UUENCODE, Unicode)으로 인코딩되거나, 압축 또는 숨겨진 파일 내에 포함되거나, 스테가노그래피를 사용하여 파일에 숨겨질 수도 있습니다. 악성 코드는 웹 액세스, 전자 메일, 전자 메일 첨부 파일, 휴대용 저장 장치 등 다양한 수단을 통해 전송될 수 있습니다. 악성 코드 삽입은 정보 시스템 취약성을 악용하여 발생합니다. 악성 코드 차단 메커니즘에는 바이러스 백신 시그니처 정의 및 평판 기반 기술 등이 포함됩니다. 악성 코드의 영향을 제한하		

제어 ID	제어 설명	AWS 구성 규칙	지침
	거나 제거하기 위한 다양한 기술과 방법이 있습니다. 광범위한 구성 관리 및 포괄적인 소프트웨어 무결성 제어는 무단 코드의 실행을 방지하는 데 효과적일 수 있습니다. 상용 소프트웨어 외에도 맞춤형 소프트웨어에도 악성 코드가 존재할 수 있습니다. 여기에는 로직 폭탄, 백도어 및 조직의 임무/비즈니스 기능에 영향을 미칠 수 있는 기타 유형의 사이버 공격 등이 포함될 수 있습니다. 기존의 악성 코드 차단 메커니즘이 이러한 코드를 항상 탐지할 수는 없습니다. 이러한 상황에서 조직은 소프트웨어가 의도한 기능 이외의 기능을 수행하지 않도록 하기 위한 보안 코딩 관행, 구성 관리 및 제어, 신뢰할 수 있는 조달 프로세스, 모니터링 관행 등 다른 보호 조치를 대신 사용합니다. 조직은 악성 코드 탐지에 대한 대응으로 다른 조치가 필요하다고 판단할 수 있습니다. 예		

제어 ID	제어 설명	AWS 구성 규칙	지침
	를 들어 조직에서는 정기 검사 중 악성 코드 탐지에 대한 대응 조치, 악성 다운로드 탐지에 대한 대응 조치 및/또는 파일을 열거나 실행하려 할 때의 악의성 탐지에 대한 대응 조치를 정의할 수 있습니다. 관련 규제 항목: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7 참고 문헌: NIST 특별 간행물 800-83.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-5	조직: a. [할당: 조직에서 정의한 외부 조직]으로부터 정보 시스템 보안 경고, 권고 및 지침을 지속적으로 받습니다. b. 필요하다고 판단되는 경우 내부 보안 경고, 권고 및 지침을 생성합니다. c. 보안 경고, 권고 및 지침을 다음에 전파합니다. [선택 (한나 이상): [할당: 조직에서 정의한 직원 또는 역할], [할당: 조직에서 정의한 조직 내 요소], [할당: 조직에서 정의한 외부 조직]] d. 정해진 일정에 따라 보안 지침을 구현하거나 발급 조직에 미준수 정도를 알립니다. 추가 지침: 미국 컴퓨터 비상 준비 팀(US-CERT)은 연방 정부 전체에 상황 인식을 유지하기 위해 보안 경고 및 권고를 생성합니다. 보안 지침은 OMB 또는 해당 지침을 발행할 책임과 권한을 가진 기타 지정 기관에서 발행합니다. 이러한 지침 중 상당수가 매우 중요하며, 지침이 적시에 시	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	행되지 않을 경우 조직 운영 및 자산, 개인, 기타 조직 및 국가에 즉각적인 악영향을 미칠 수 있기 때문에 보안 지침을 준수하는 것이 필수적입니다. 외부 조직에는 예를 들어 외부 미션/비즈니스 파트너, 공급망 파트너, 외부 서비스 제공업체 및 기타 동료/지원 조직이 포함됩니다. 관련 통제: SI-2. 참고 문헌: NIST 특별 간행물 800-40.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-5	조직: a. [할당: 조직에서 정의한 외부 조직]으로부터 정보 시스템 보안 경고, 권고 및 지침을 지속적으로 받습니다. b. 필요하다고 판단되는 경우 내부 보안 경고, 권고 및 지침을 생성합니다. c. 보안 경고, 권고 및 지침을 다음에 전파합니다. [선택 (한나 이상): [할당: 조직에서 정의한 직원 또는 역할], [할당: 조직에서 정의한 조직 내 요소], [할당: 조직에서 정의한 외부 조직]] d. 정해진 일정에 따라 보안 지침을 구현하거나 발급 조직에 미준수 정도를 알립니다. 추가 지침: 미국 컴퓨터 비상 준비 팀(US-CERT)은 연방 정부 전체에 상황 인식을 유지하기 위해 보안 경고 및 권고를 생성합니다. 보안 지침은 OMB 또는 해당 지침을 발행할 책임과 권한을 가진 기타 지정 기관에서 발행합니다. 이러한 지침 중 상당수가 매우 중요하며, 지침이 적시에 시	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	행되지 않을 경우 조직 운영 및 자산, 개인, 기타 조직 및 국가에 즉각적인 악영향을 미칠 수 있기 때문에 보안 지침을 준수하는 것이 필수적입니다. 외부 조직에는 예를 들어 외부 미션/비즈니스 파트너, 공급망 파트너, 외부 서비스 제공업체 및 기타 동료/지원 조직이 포함됩니다. 관련 통제: SI-2. 참고 문헌: NIST 특별 간행물 800-40.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-5	조직: a. [할당: 조직에서 정의한 외부 조직]으로부터 정보 시스템 보안 경고, 권고 및 지침을 지속적으로 받습니다. b. 필요하다고 판단되는 경우 내부 보안 경고, 권고 및 지침을 생성합니다. c. 보안 경고, 권고 및 지침을 다음에 전파합니다. [선택 (한나 이상): [할당: 조직에서 정의한 직원 또는 역할], [할당: 조직에서 정의한 조직 내 요소], [할당: 조직에서 정의한 외부 조직]] d. 정해진 일정에 따라 보안 지침을 구현하거나 발급 조직에 미준수 정도를 알립니다. 추가 지침: 미국 컴퓨터 비상 준비 팀(US-CERT)은 연방 정부 전체에 상황 인식을 유지하기 위해 보안 경고 및 권고를 생성합니다. 보안 지침은 OMB 또는 해당 지침을 발행할 책임과 권한을 가진 기타 지정 기관에서 발행합니다. 이러한 지침 중 상당수가 매우 중요하며, 지침이 적시에 시	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	행되지 않을 경우 조직 운영 및 자산, 개인, 기타 조직 및 국가에 즉각적인 악영향을 미칠 수 있기 때문에 보안 지침을 준수하는 것이 필수적입니다. 외부 조직에는 예를 들어 외부 미션/비즈니스 파트너, 공급망 파트너, 외부 서비스 제공업체 및 기타 동료/지원 조직이 포함됩니다. 관련 통제: SI-2. 참고 문헌: NIST 특별 간행물 800-40.		

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-5	조직: a. [할당: 조직에서 정의한 외부 조직]으로부터 정보 시스템 보안 경고, 권고 및 지침을 지속적으로 받습니다. b. 필요하다고 판단되는 경우 내부 보안 경고, 권고 및 지침을 생성합니다. c. 보안 경고, 권고 및 지침을 다음에 전파합니다. [선택 (한나 이상): [할당: 조직에서 정의한 직원 또는 역할], [할당: 조직에서 정의한 조직 내 요소], [할당: 조직에서 정의한 외부 조직]] d. 정해진 일정에 따라 보안 지침을 구현하거나 발급 조직에 미준수 정도를 알립니다. 추가 지침: 미국 컴퓨터 비상 준비 팀(US-CERT)은 연방 정부 전체에 상황 인식을 유지하기 위해 보안 경고 및 권고를 생성합니다. 보안 지침은 OMB 또는 해당 지침을 발행할 책임과 권한을 가진 기타 지정 기관에서 발행합니다. 이러한 지침 중 상당수가 매우 중요하며, 지침이 적시에 시	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	행되지 않을 경우 조직 운영 및 자산, 개인, 기타 조직 및 국가에 즉각적인 악영향을 미칠 수 있기 때문에 보안 지침을 준수하는 것이 필수적입니다. 외부 조직에는 예를 들어 외부 미션/비즈니스 파트너, 공급망 파트너, 외부 서비스 제공업체 및 기타 동료/지원 조직이 포함됩니다. 관련 통제: SI-2. 참고 문헌: NIST 특별 간행물 800-40.		
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
AU-12(a)(c)	정보 시스템: a. 감사 기능이 배포된/사용 가능한 모든 정보 시스템 및 네트워크 구성 요소에서 AU-2 a.에 정의된 감사 가능한 이벤트에 대한 감사 레코드 생성 기능을 제공합니다. c. AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2(a)(d)	조직: a. 정보 시스템이 성공 및 실패한 계정 로그온 이벤트, 계정 관리 이벤트, 객체 액세스, 정책 변경, 권한 기능, 프로세스 추적, 시스템 이벤트 등의 이벤트를 감사할 수 있는지 확인합니다. 웹 애플리케이션의 경우: 모든 관리자 활동, 인증 검사, 권한 부여 검사, 데이터 삭제, 데이터 액세스, 데이터 변경, 권한 변경. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [AU-2 a에 정의된 감사 가능 이벤트 중 조직이 정의한 하위 집합을 식별된 각 이벤트에 대해 지속적으로 감사해야 함].	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

템플릿

템플릿은 GitHub: FedRAMP(High 파트 1) 운영 모범 사례에서 확인할 수 있습니다.

FedRAMP(High 파트 2) 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제

공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 연방 위험 및 권한 부여 관리 프로그램(FedRAMP)과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 FedRAMP 제어와 관련이 있습니다. FedRAMP 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-02(11)	정보 시스템은 조직 정의 환경 및/또는 사용 조건을 조직 정의 시스템 계정에 적용합니다.	guardduty-enabled-centralized	Amazon GuardDuty를 사용하여 IAM 인스턴스 역할과 연결된 단기 보안 인증 정보 사용을 모니터링합니다. Amazon GuardDuty는 UnauthorizedAccess 확인을 사용하여 IAM 인스턴스 프로파일에서 보안 인증 정보 유출을 확인할 수 있습니다.
AC-02(12)(a)	조직: a. 정보 시스템 계정의 [할당: 조직에서 정의한 비정형 용도] 활동을 모니터링합니다.	cloudtrail-security-trail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코

제어 ID	제어 설명	AWS 구성 규칙	지침
			드 콘텐츠에서 확인할 수 있습니다.
AC-06(03)	조직은 보안 계획에 대한 액세스 작업을 완료해야 하는 경우에만 할당된 직원에 대한 네트워크 액세스를 승인합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
AC-06(03)	조직은 [할당: 조직에서 정의한 권한이 있는 명령]에 대한 네트워크 액세스를 [할당: 조직에서 정의한 필수 운영 요구 사항]에 대해서만 승인하고 이러한 액세스의 이론적 근거를 시스템의 보안 계획에 문서화합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-06(03)	조직은 [할당: 조직에서 정의한 권한이 있는 명령]에 대한 네트워크 액세스를 [할당: 조직에서 정의한 필수 운영 요구 사항]에 대해서만 승인하고 이러한 액세스의 이론적 근거를 시스템의 보안 계획에 문서화합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
AC-06(03)	조직은 [할당: 조직에서 정의한 권한이 있는 명령]에 대한 네트워크 액세스를 [할당: 조직에서 정의한 필수 운영 요구 사항]에 대해서만 승인하고 이러한 액세스의 이론적 근거를 시스템의 보안 계획에 문서화합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-06(03)	조직은 [할당: 조직에서 정의한 권한이 있는 명령]에 대한 네트워크 액세스를 [할당: 조직에서 정의한 필수 운영 요구 사항]에 대해서만 승인하고 이러한 액세스의 이론적 근거를 시스템의 보안 계획에 문서화합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-06(03)	조직은 [할당: 조직에서 정의한 권한이 있는 명령]에 대한 네트워크 액세스를 [할당: 조직에서 정의한 필수 운영 요구 사항]에 대해서만 승인하고 이러한 액세스의 이론적 근거를 시스템의 보안 계획에 문서화합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-06(03)	조직은 [할당: 조직에서 정의한 권한이 있는 명령]에 대한 네트워크 액세스를 [할당: 조직에서 정의한 필수 운영 요구 사항]에 대해서만 승인하고 이러한 액세스의 이론적 근거를 시스템의 보안 계획에 문서화합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-06(03)	조직은 [할당: 조직에서 정의한 권한이 있는 명령]에 대한 네트워크 액세스를 [할당: 조직에서 정의한 필수 운영 요구 사항]에 대해서만 승인하고 이러한 액세스의 이론적 근거를 시스템의 보안 계획에 문서화합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-06(03)	조직은 [할당: 조직에서 정의한 권한이 있는 명령]에 대한 네트워크 액세스를 [할당: 조직에서 정의한 필수 운영 요구 사항]에 대해서만 승인하고 이러한 액세스의 이론적 근거를 시스템의 보안 계획에 문서화합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC-06(03)	조직은 [할당: 조직에서 정의한 권한이 있는 명령]에 대한 네트워크 액세스를 [할당: 조직에서 정의한 필수 운영 요구 사항]에 대해서만 승인하고 이러한 액세스의 이론적 근거를 시스템의 보안 계획에 문서화합니다.	eks-endpoint-no-public-access	Kubernetes API 서버 엔드포인트에 공개적으로 액세스할 수 없도록 하여 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 대한 액세스를 관리합니다. Kubernetes API 서버 엔드포인트에 대한 퍼블릭 액세스를 제한하면 EKS 클러스터 및 해당 리소스에 대한 무단 액세스 위험을 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-05(02)	정보 시스템은 할당된 감사 로그 스토리지 볼륨이 리포지토리 최대 감사 로그 스토리지 용량의 설정된 백분율에 도달하면 설정된 시간 내에 담당자에게 경고합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-06(04)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-06(05)	조직은 감사 기록 분석을 취약성 스캔 정보, 성능 데이터 및 시스템 모니터링 정보 분석과 통합하여 부적절하거나 비정상적인 활동을 식별하는 기능을 더욱 강화합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-06(05)	조직은 감사 기록 분석을 [선택(하나 이상): 취약성 스캔 정보, 성능 데이터, 시스템 모니터링 정보, [할당: 다른 소스에서 수집한 조직 정의 데이터/정보]]의 분석과 통합하여 부적절하거나 비정상적인 활동을 식별하는 기능을 더욱 강화합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-06(07)	조직은 감사 기록 정보의 검토, 분석 및 보고와 관련된 각 시스템 프로세스, 역할 및 사용자에 허용하는 작업을 지정합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AU-06(07)	조직은 감사 기록 정보의 검토, 분석 및 보고와 관련된 각 [선택(하나 이상): 시스템 프로세스, 역할, 사용자]에 허용하는 작업을 지정합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-09(02)	정보 시스템은 감사 정보 및 감사 도구의 무결성을 보호하기 위해 암호화 메커니즘을 구현합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
AU-09(02)	정보 시스템은 감사 정보 및 감사 도구의 무결성을 보호하기 위해 암호화 메커니즘을 구현합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-09(02)	정보 시스템은 감사 정보 및 감사 도구의 무결성을 보호하기 위해 암호화 메커니즘을 구현합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
AU-09(02)	정보 시스템은 감사 정보 및 감사 도구의 무결성을 보호하기 위해 암호화 메커니즘을 구현합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-09(03)	정보 시스템은 개인이 수행한 반박할 수 없는 증거를 제공합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
AU-09(03)	정보 시스템은 감사 로그 데이터에 대한 네트워크 액세스를 제한합니다.	cloudtrail-s3-bucket-public-access-prohibited	CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–10	정보 시스템은 개인(또는 개인을 대신하여 조취를 취하는 프로스세)이 [할당: 거부 금지가 적용되는 조직이 정의한 작업]을 수행했다는 반박할 수 없는 증거를 제공합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU–10	정보 시스템은 개인(또는 개인을 대신하여 조취를 취하는 프로스세)이 [할당: 거부 금지가 적용되는 조직이 정의한 작업]을 수행했다는 반박할 수 없는 증거를 제공합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–10	정보 시스템은 개인(또는 개인을 대신하여 조취를 취하는 프로스세)이 [할당: 거부 금지가 적용되는 조직이 정의한 작업]을 수행했다는 반박할 수 없는 증거를 제공합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	조직은 [할당: 조직이 정의한 시스템 구성 요소]의 감사 기록을 [할당: 감사 추적에서 조직이 정의한 개별 기록의 타임스탬프 간 관계의 허용 오차 수준] 내에서 시간과 관련된 시스템 전체(논리적 또는 물리적) 감사 추적으로 컴파일합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU–12	조직은 [할당: 조직이 정의한 시스템 구성 요소]의 감사 기록을 [할당: 감사 추적에서 조직이 정의한 개별 기록의 타임스탬프 간 관계의 허용 오차 수준] 내에서 시간과 관련된 시스템 전체(논리적 또는 물리적) 감사 추적으로 컴파일합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	조직은 [할당: 조직이 정의한 시스템 구성 요소]의 감사 기록을 [할당: 감사 추적에서 조직이 정의한 개별 기록의 타임스탬프 간 관계의 허용 오차 수준] 내에서 시간과 관련된 시스템 전체(논리적 또는 물리적) 감사 추적으로 컴파일합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.
AU–12	조직은 [할당: 조직이 정의한 시스템 구성 요소]의 감사 기록을 [할당: 감사 추적에서 조직이 정의한 개별 기록의 타임스탬프 간 관계의 허용 오차 수준] 내에서 시간과 관련된 시스템 전체(논리적 또는 물리적) 감사 추적으로 컴파일합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	조직은 [할당: 조직이 정의한 시스템 구성 요소]의 감사 기록을 [할당: 감사 추적에서 조직이 정의한 개별 기록의 타임스탬프 간 관계의 허용 오차 수준] 내에서 시간과 관련된 시스템 전체(논리적 또는 물리적) 감사 추적으로 컴파일합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	조직은 [할당: 조직이 정의한 시스템 구성 요소]의 감사 기록을 [할당: 감사 추적에서 조직이 정의한 개별 기록의 타임스탬프 간 관계의 허용 오차 수준] 내에서 시간과 관련된 시스템 전체(논리적 또는 물리적) 감사 추적으로 컴파일합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
AU–12	조직은 [할당: 조직이 정의한 시스템 구성 요소]의 감사 기록을 [할당: 감사 추적에서 조직이 정의한 개별 기록의 타임스탬프 간 관계의 허용 오차 수준] 내에서 시간과 관련된 시스템 전체(논리적 또는 물리적) 감사 추적으로 컴파일합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU–12	조직은 [할당: 조직이 정의한 시스템 구성 요소]의 감사 기록을 [할당: 감사 추적에서 조직이 정의한 개별 기록의 타임스탬프 간 관계의 허용 오차 수준] 내에서 시간과 관련된 시스템 전체(논리적 또는 물리적) 감사 추적으로 컴파일합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
AU–12	조직은 [할당: 조직이 정의한 시스템 구성 요소]의 감사 기록을 [할당: 감사 추적에서 조직이 정의한 개별 기록의 타임스탬프 간 관계의 허용 오차 수준] 내에서 시간과 관련된 시스템 전체(논리적 또는 물리적) 감사 추적으로 컴파일합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-03	조직은 구성을 제어하는 시스템의 변경 유형을 결정하고 문서화합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CM-08(02)	조직은 [할당: 조직이 정의한 자동화 메커니즘]을 사용하여 시스템 구성 요소 인벤토리의 통용, 완전성, 정확성 및 가용성을 유지합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-08(02)	조직은 [할당: 조직이 정의한 자동화 메커니즘]을 사용하여 시스템 구성 요소 인벤토리의 통용, 완전성, 정확성 및 가용성을 유지합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
CM-08(02)	조직은 [할당: 조직이 정의한 자동화 메커니즘]을 사용하여 시스템 구성 요소 인벤토리의 통용, 완전성, 정확성 및 가용성을 유지합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-02(05)	조직은 운영 연속성의 손실을 최소화 또는 제로화하여 미션 및 비즈니스 기능의 연속성을 위한 계획을 제공하고 기본 처리 및/또는 스토리지 사이트에서 전체 시스템 복원까지 해당 연속성을 유지합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	backup-recovery-point-minimum-retention-check	지정된 기간 이후보다 복구 시점이 더 빨리 만료되지 않는지 확인합니다. 조직은 비상 계획의 일환으로 복구 시간 및 복구 시점 목표를 설정합니다. 대체 스토리지 사이트의 구성에는 물리적 시설과 접근성과 올바른 실행을 보장하는 복구 작업을 지원하는 시스템이 포함됩니다.
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	rds-in-backup-plan	AWS 백업 계획에 Amazon Relational Database Service(Amazon RDS) 데이터베이스가 있는지 확인합니다. 조직은 비상 계획의 일환으로 복구 시간 및 복구 시점 목표를 설정합니다. 대체 스토리지 사이트의 구성에는 물리적 시설과 접근성과 올바른 실행을 보장하는 복구 작업을 지원하는 시스템이 포함됩니다.
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	dynamodb-in-backup-plan	Amazon DynamoDB 테이블이 AWS 백업 계획에 있는지 확인합니다. 조직은 비상 계획의 일환으로 복구 시간 및 복구 시점 목표를 설정합니다. 대체 스토리지 사이트의 구성에는 물리적 시설과 접근성과 올바른 실행을 보장하는 복구 작업을 지원하는 시스템이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-06(02)	조직은 복구 시간 및 복구 시점 목표에 따라 복구 작업을 용이하게 하도록 대체 스토리지 사이트를 구성합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-07(01)	조직은 동일한 위협에 대한 취약성을 줄이기 위해 기본 처리 사이트와 충분히 분리된 대체 처리 사이트를 식별합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-07(04)	조직은 대체 처리 사이트를 준비하여 사이트가 필수 미션 및 비즈니스 기능을 지원하는 운영 사이트 역할을 할 수 있도록 합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-07(04)	조직은 대체 처리 사이트를 준비하여 사이트가 필수 미션 및 비즈니스 기능을 지원하는 운영 사이트 역할을 할 수 있도록 합니다.	backup-recovery-point-encrypted	복구 시점이 암호화되어 있는지 확인합니다. 사이트 준비에는 대체 처리 사이트의 시스템에 대한 구성 설정을 기본 사이트의 해당 설정에 대한 요구 사항에 맞게 설정하고 필수 공급 및 물류 고려 사항이 마련되어 있는지 확인하는 것이 포함됩니다.
CP-07(04)	조직은 대체 처리 사이트를 준비하여 사이트가 필수 미션 및 비즈니스 기능을 지원하는 운영 사이트 역할을 할 수 있도록 합니다.	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 사이트 준비에는 대체 처리 사이트의 시스템에 대한 구성 설정을 기본 사이트의 해당 설정에 대한 요구 사항에 맞게 설정하고 필수 공급 및 물류 고려 사항이 마련되어 있는지 확인하는 것이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-07(04)	조직은 대체 처리 사이트를 준비하여 사이트가 필수 미션 및 비즈니스 기능을 지원하는 운영 사이트 역할을 할 수 있도록 합니다.	s3-bucket-cross-region-replication-enabled	Amazon S3 버킷에 대해 S3 교차 리전 복제를 활성화했는지 확인합니다. 사이트 준비에는 대체 처리 사이트의 시스템에 대한 구성 설정을 기본 사이트의 해당 설정에 대한 요구 사항에 맞게 설정하고 필수 공급 및 물류 고려 사항이 마련되어 있는지 확인하는 것이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-09(03)	조직은 [할당: 조직에서 정의한 중요 시스템 소프트웨어 및 기타 보안 관련 정보]의 백업 사본을 별도의 시설 또는 운영 체제와 함께 배치되지 않은 화재 등급 컨테이너에 저장합니다.	backup-recovery-point-minimum-retention-check	지정된 기간 이후보다 복구 시점이 더 빨리 만료되지 않는지 확인합니다. 백업 스토리지 미디어의 유형에 관계없이 중요 정보를 위한 별도의 스토리지가 모든 중요 정보에 적용됩니다. 중요 시스템 소프트웨어에는 운영 체제, 미들웨어, 암호화 키 관리 시스템 및 침입 탐지 시스템이 포함됩니다. 보안 관련 정보에는 시스템 하드웨어, 소프트웨어 및 펌웨어 구성 요소의 인벤토리가 포함됩니다. 지리적으로 분산된 아키텍처를 포함한 대체 스토리지 사이트는 조직을 위한 별도의 스토리지 시설 역할을 합니다. 조직은 대체 스토리지 사이트(예: 데이터 센터)에서 자동 백업 프로세스를 구현하여 별도의 스토리지를 제공할 수 있습니다. General Services Administration(GSA)은 보안 및 화재 등급 컨테이너에 대한 표준과 사양을 설정합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-09(03)	조직은 [할당: 조직에서 정의한 중요 시스템 소프트웨어 및 기타 보안 관련 정보]의 백업 사본을 별도의 시설 또는 운영 체제와 함께 배치되지 않은 화재 등급 컨테이너에 저장합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-09(03)	조직은 [할당: 조직에서 정의한 중요 시스템 소프트웨어 및 기타 보안 관련 정보]의 백업 사본을 별도의 시설 또는 운영 체제와 함께 배치되지 않은 화재 등급 컨테이너에 저장합니다.	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-09(03)	조직은 [할당: 조직에서 정의한 중요 시스템 소프트웨어 및 기타 보안 관련 정보]의 백업 사본을 별도의 시설 또는 운영 체제와 함께 배치되지 않은 화재 등급 컨테이너에 저장합니다.	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-09(03)	조직은 [할당: 조직에서 정의한 중요 시스템 소프트웨어 및 기타 보안 관련 정보]의 백업 사본을 별도의 시설 또는 운영 체제와 함께 배치되지 않은 화재 등급 컨테이너에 저장합니다.	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-09(03)	조직은 [할당: 조직에서 정의한 중요 시스템 소프트웨어 및 기타 보안 관련 정보]의 백업 사본을 별도의 시설 또는 운영 체제와 함께 배치되지 않은 화재 등급 컨테이너에 저장합니다.	s3-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Simple Storage Service(Amazon S3) 버킷이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-09(03)	조직은 [할당: 조직에서 정의한 중요 시스템 소프트웨어 및 기타 보안 관련 정보]의 백업 사본을 별도의 시설 또는 운영 체제와 함께 배치되지 않은 화재 등급 컨테이너에 저장합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-09(03)	조직은 [할당: 조직에서 정의한 중요 시스템 소프트웨어 및 기타 보안 관련 정보]의 백업 사본을 별도의 시설 또는 운영 체제와 함께 배치되지 않은 화재 등급 컨테이너에 저장합니다.	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-09(03)	조직은 [할당: 조직에서 정의한 중요 시스템 소프트웨어 및 기타 보안 관련 정보]의 백업 사본을 별도의 시설 또는 운영 체제와 함께 배치되지 않은 화재 등급 컨테이너에 저장합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-09(03)	조직은 [할당: 조직에서 정의한 중요 시스템 소프트웨어 및 기타 보안 관련 정보]의 백업 사본을 별도의 시설 또는 운영 체제와 함께 배치되지 않은 화재 등급 컨테이너에 저장합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-09(05)	조직은 시스템 백업 정보를 대체 스토리지 사이트[할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 기간 및 전송 속도]로 전송합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-09(05)	조직은 시스템 백업 정보를 대체 스토리지 사이트[할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 기간 및 전송 속도]로 전송합니다.	backup-recovery-point-minimum-retention-check	지정된 기간 이후보다 복구 시점이 더 빨리 만료되지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-09(05)	조직은 시스템 백업 정보를 대체 스토리지 사이트[할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 기간 및 전송 속도]로 전송합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-09(05)	조직은 시스템 백업 정보를 대체 스토리지 사이트[할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 기간 및 전송 속도]로 전송합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-09(05)	조직은 시스템 백업 정보를 대체 스토리지 사이트[할당: 복구 시간 및 복구 시점 목표와 일치하는 조직 정의 기간 및 전송 속도]로 전송합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-09(08)	조직은 암호화 메커니즘을 사용하여 무단 공개 백업 정보를 방지합니다.	backup-recovery-point-encrypted	백업 정보의 기밀성과 무결성 보호에 대한 요구사항에 따라 암호화 메커니즘을 선택합니다. 선택한 메커니즘의 강도는 정보의 보안 범주 또는 분류에 상응합니다. 암호화 보호는 기본 및 대체 위치 모두에서 스토리지의 시스템 백업 정보에 적용됩니다. 정보를 보호하기 위해 암호화 메커니즘을 구현하는 조직도 암호화 키 관리 솔루션을 고려합니다.
CP-10(04)	조직은 구성이 제어되고 무결성이 보호된 구성 요소의 알려진 작동 상태를 나타내는 정보로부터 [할당: 조직이 정의한 복원 기간] 이내에 시스템 구성 요소를 복원할 수 있는 기능을 제공합니다.	backup-recovery-point-encrypted	복구 시점이 암호화되었는지 확인하려면 이 규칙을 활성화합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10(04)	조직은 구성이 제어되고 무결성이 보호된 구성 요소의 알려진 작동 상태를 나타내는 정보로부터 [할당: 조직이 정의한 복원 기간] 이내에 시스템 구성 요소를 복원할 수 있는 기능을 제공합니다.	backup-recovery-point-minimum-retention-check	지정된 기간 이후에 복구 시점이 만료되지 않도록 하려면 이 규칙을 활성화합니다.
CP-10(04)	조직은 구성이 제어되고 무결성이 보호된 구성 요소의 알려진 작동 상태를 나타내는 정보로부터 [할당: 조직이 정의한 복원 기간] 이내에 시스템 구성 요소를 복원할 수 있는 기능을 제공합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
CP-10(04)	조직은 구성이 제어되고 무결성이 보호된 구성 요소의 알려진 작동 상태를 나타내는 정보로부터 [할당: 조직이 정의한 복원 기간] 이내에 시스템 구성 요소를 복원할 수 있는 기능을 제공합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10(04)	조직은 구성이 제어되고 무결성이 보호된 구성 요소의 알려진 작동 상태를 나타내는 정보로부터 [할당: 조직이 정의한 복원 기간] 이내에 시스템 구성 요소를 복원할 수 있는 기능을 제공합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
IA-02(02)	권한 없는 계정에 대한 액세스를 위한 다중 인증을 구현합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-02(02)	권한 없는 계정에 대한 액세스를 위한 다중 인증을 구현합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-02(06)	정보 시스템은 [선택(하나 이상): 권한 있는 계정, 권한이 없는 계정]에 대한 [선택(하나 이상): 로컬, 네트워크, 원격] 액세스를 위한 다중 인증을 구현합니다. (a)인증 요소 중 하나는 액세스 권한을 얻는 시스템과 분리된 장치에서 제공하고 (b)해당 장치는 [할당: 조직이 정의한 메커니즘 강도 요구 사항]을 충족합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-02(06)	정보 시스템은 [선택(하나 이상): 권한 있는 계정, 권한이 없는 계정]에 대한 [선택(하나 이상): 로컬, 네트워크, 원격] 액세스를 위한 다중 인증을 구현합니다. (a)인증 요소 중 하나는 액세스 권한을 얻는 시스템과 분리된 장치에서 제공하고 (b)해당 장치는 [할당: 조직이 정의한 메커니즘 강도 요구 사항]을 충족합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-02(08)	정보 시스템은 [선택(하나 이상): 권한 있는 계정, 권한이 없는 계정]에 대한 액세스를 위한 재생 방지 인증 메커니즘을 구현합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-05(08)	정보 시스템은 [할당: 조직이 정의한 보안 제어]를 구현하여 여러 시스템에 계정이 있는 개인으로 인한 침해 위험을 관리합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IA-05(08)	정보 시스템은 [할당: 조직이 정의한 보안 제어]를 구현하여 여러 시스템에 계정이 있는 개인으로 인한 침해 위험을 관리합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
IA-05(08)	정보 시스템은 [할당: 조직이 정의한 보안 제어]를 구현하여 여러 시스템에 계정이 있는 개인으로 인한 침해 위험을 관리합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정을 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-05(08)	정보 시스템은 [할당: 조직이 정의한 보안 제어]를 구현하여 여러 시스템에 계정이 있는 개인으로 인한 침해 위험을 관리합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-05(08)	정보 시스템은 [할당: 조직이 정의한 보안 제어]를 구현하여 여러 시스템에 계정이 있는 개인으로 인한 침해 위험을 관리합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
IA-05(08)	정보 시스템은 [할당: 조직이 정의한 보안 제어]를 구현하여 여러 시스템에 계정이 있는 개인으로 인한 침해 위험을 관리합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 IAM 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-04(04)	조직은 자동화된 메커니즘을 사용하여 인시던트 정보와 개별 인시던트 응답을 상호 연관시켜 인시던트 인식 및 대응에 대한 조직 전반의 관점을 달성합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-04(04)	조직은 자동화된 메커니즘을 사용하여 인시던트 정보와 개별 인시던트 응답을 상호 연관시켜 인시던트 인식 및 대응에 대한 조직 전반의 관점을 달성합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
IR-04(04)	조직은 자동화된 메커니즘을 사용하여 인시던트 정보와 개별 인시던트 응답을 상호 연관시켜 인시던트 인식 및 대응에 대한 조직 전반의 관점을 달성합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-04(04)	조직은 자동화된 메커니즘을 사용하여 인시던트 정보와 개별 인시던트 응답을 상호 연관시켜 인시던트 인식 및 대응에 대한 조직 전반의 관점을 달성합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
IR-04(04)	조직은 자동화된 메커니즘을 사용하여 인시던트 정보와 개별 인시던트 응답을 상호 연관시켜 인시던트 인식 및 대응에 대한 조직 전반의 관점을 달성합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-05	취약성 호스팅 애플리케이션을 모니터링하고 스캔하며 시스템에 잠재적으로 영향을 미칠 수 있는 새 취약성을 식별하고 보고합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
RA-05	취약성 스캔 적용 범위의 폭과 깊이를 정의합니다.	inspector-lambda-standard-scan-enabled	단일 또는 다중 계정 환경에 대해 Amazon Inspector V2 Lambda 표준 스캔이 활성화되어 잠재적 소프트웨어 취약성을 감지하는지 확인합니다. Lambda 표준 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-05	취약성 스캔 적용 범위의 폭과 깊이를 정의합니다.	inspector-ec2-scan-enabled	단일 또는 다중 계정 환경에 대해 Amazon Inspector V2 EC2 스캔이 활성화되어 EC2 인스턴스의 잠재적 취약성 및 네트워크 연결성 문제를 감지하는지 확인합니다. EC2 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
RA-05	취약성 스캔 적용 범위의 폭과 깊이를 정의합니다.	inspector-ecr-scan-enabled	단일 또는 다중 계정 환경에 대해 Amazon Inspector V2 ECR 스캔이 활성화되어 컨테이너 이미지의 잠재적 소프트웨어 취약성을 감지하는지 확인합니다. ECR 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-05(03)	취약성 스캔 적용 범위의 폭과 깊이를 정의합니다.	inspector-lambda-standard-scan-enabled	단일 또는 다중 계정 환경에 대해 Amazon Inspector V2 Lambda 표준 스캔이 활성화되어 잠재적 소프트웨어 취약성을 감지하는지 확인합니다. Lambda 표준 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
RA-05(03)	취약성 스캔 적용 범위의 폭과 깊이를 정의합니다.	inspector-ec2-scan-enabled	단일 또는 다중 계정 환경에 대해 Amazon Inspector V2 EC2 스캔이 활성화되어 EC2 인스턴스의 잠재적 취약성 및 네트워크 연결성 문제를 감지하는지 확인합니다. EC2 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-05(03)	취약성 스캔 적용 범위의 폭과 깊이를 정의합니다.	inspector-ecr-scan-enabled	단일 또는 다중 계정 환경에 대해 Amazon Inspector V2 ECR 스캔이 활성화되어 컨테이너 이미지의 잠재적 소프트웨어 취약성을 감지하는지 확인합니다. ECR 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT 입니다.
RA-05(05)	조직의 스캔에 대해 [할당: 조직 정의 시스템 구성 요소]에 대한 권한 있는 액세스 권한을 구현합니다. (인증 및 모든 스캔을 지원하는 모든 구성 요소를 지정합니다.)	inspector-ec2-scan-enabled	단일 또는 다중 계정 환경에 대해 Amazon Inspector V2 EC2 스캔이 활성화되어 EC2 인스턴스의 잠재적 취약성 및 네트워크 연결성 문제를 감지하는지 확인합니다. EC2 스캔이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10	조직은 시스템, 시스템 구성 요소 또는 시스템 서비스 개발자에게 다음을 요구합니다. a. 시스템, 구성 요소 또는 서비스의 [선택(하나 이상): 설계, 개발, 구현, 운영, 폐기] 중 구성 관리 수행 b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 및 개인정보 보호 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-07(12)	조직은 [할당: 조직 정의 시스템 구성 요소]에서 [할당: 조직 정의 호스트 기반 경계 보호 메커니즘]을 구현합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-07(20)	[할당: 조직 정의 시스템 구성 요소]를 다른 시스템 구성 요소에서 동적으로 격리할 수 있는 기능을 제공합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-07(21)	경계 보호 메커니즘을 사용하여 [할당: 조직 정의 미션 및/또는 비즈니스 기능]을 지원하는 [할당: 조직 정의 시스템 구성 요소]를 격리합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-07(21)	경계 보호 메커니즘을 사용하여 [할당: 조직 정의 미션 및/또는 비즈니스 기능]을 지원하는 [할당: 조직 정의 시스템 구성 요소]를 격리합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-12(01)	키 관리 요구사항([할당: 키 생성, 배포, 저장, 액세스 및 폐기에 대해 조직이 정의한 요구 사항])에 따라 시스템 내에서 암호화를 사용할 때 암호화 키를 설정하고 관리합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(01)	조직은 [할당: 조직 정의 시스템 구성 요소 또는 미디어]: [할당: 조직 정의 정보]에 저장된 다음 정보의 무단 공개 및 수정을 방지하기 위해 암호화 메커니즘을 구현합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-04(12)	[할당: 경보를 트리거하는 조직 정의 활동]과 같은 보안 또는 개인정보 보호에 영향을 미치는 부적절하거나 비정상적인 활동이 발생할 경우 [할당: 조직이 정의한 자동화 메커니즘]을 사용하여 [할당: 조직 정의 인력 또는 역할]에 경보를 보냅니다.	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.
SI-04(20)	권한 있는 사용자에 대해 [할당: 조직 정의 추가 모니터링]을 추가로 모니터링합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-04(20)	권한 있는 사용자에 대해 [할당: 조직 정의 추가 모니터링]을 추가로 모니터링합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-04(20)	권한 있는 사용자에 대해 [할당: 조직 정의 추가 모니터링]을 추가로 모니터링합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-04(20)	권한 있는 사용자에 대해 [할당: 조직 정의 추가 모니터링]을 추가로 모니터링합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 AWS 계정 내 API 호출 활동에 대한 세부 정보가 제공됩니다.
SI-04(20)	권한 있는 사용자에 대해 [할당: 조직 정의 추가 모니터링]을 추가로 모니터링합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-04(20)	권한 있는 사용자에 대해 [할당: 조직 정의 추가 모니터링]을 추가로 모니터링합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
SI-04(20)	권한 있는 사용자에 대해 [할당: 조직 정의 추가 모니터링]을 추가로 모니터링합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-04(20)	권한 있는 사용자에 대해 [할당: 조직 정의 추가 모니터링]을 추가로 모니터링합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-04(20)	권한 있는 사용자에 대해 [할당: 조직 정의 추가 모니터링]을 추가로 모니터링합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-04(22)	(a) [할당: 조직 정의 권한 부여 또는 승인 프로세스]에서 승인 또는 승인하지 않은 네트워크 서비스를 탐지하고, (b) [선택(하나 이상): 감사, [할당: 조직 정의 직원 또는 역할]]이 탐지되면 이를 알립니다.	securityhub-enabled	(A) AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-04(22)	(a) [할당: 조직 정의 권한 부여 또는 승인 프로세스]에서 승인 또는 승인하지 않은 네트워크 서비스를 탐지하고, (b) [선택(하나 이상): 감사, [할당: 조직 정의 직원 또는 역할]]이 탐지되면 이를 알립니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
SI-04(22)	(a) [할당: 조직 정의 권한 부여 또는 승인 프로세스]에서 승인 또는 승인하지 않은 네트워크 서비스를 탐지하고, (b) [선택(하나 이상): 감사, [할당: 조직 정의 직원 또는 역할]]이 탐지되면 이를 알립니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-05(01)	[할당: 조직이 정의한 자동화 메커니즘]을 사용하여 조직 전체에 보안 알림 및 권고 정보를 브로드캐스트합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-05(01)	[할당: 조직이 정의한 자동화 메커니즘]을 사용하여 조직 전체에 보안 알림 및 권고 정보를 브로드캐스트합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-07(02)	무결성 확인 중에 불일치를 발견하면 [할당: 조직 정의 직원 또는 역할]에 알림을 제공하는 자동 도구를 사용합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI-07(02)	무결성 확인 중에 불일치를 발견하면 [할당: 조직 정의 직원 또는 역할]에 알림을 제공하는 자동 도구를 사용합니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-07(05)	무결성 위반이 발견되면 자동으로 [선택(하나 이상): 시스템 종료, 시스템 재시작, [할당: 조직 정의 제어] 구현]을 수행합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
SI-07(05)	무결성 위반이 발견되면 자동으로 [선택(하나 이상): 시스템 종료, 시스템 재시작, [할당: 조직 정의 제어] 구현]을 수행합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-07(15)	설치 전에 [할당: 조직 정의 소프트웨어 또는 펌웨어 구성 요소]와 같은 소프트웨어 또는 펌웨어 구성 요소를 인증하는 암호화 메커니즘을 구현합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
SI-07(15)	설치 전에 [할당: 조직 정의 소프트웨어 또는 펌웨어 구성 요소]와 같은 소프트웨어 또는 펌웨어 구성 요소를 인증하는 암호화 메커니즘을 구현합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

템플릿

템플릿은 GitHub: FedRAMP(High 파트 2) 운영 모범 사례에서 확인할 수 있습니다.

FFIEC 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 연방 금융 기관 검사 위원회(FFIEC) 사이버 보안 평가 도구 도메인과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 FFIEC 사이버 보안 평가 도구 제어와 관련이 있습니다. FFIEC 사이버 보안 평가 도구 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
D1.G.IT.B.1	조직 자산(예: 외부적으로 호스팅되는 하드웨어, 소프트웨어, 데이터 및 시스템)의 인벤토리가 유지 관리됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
D1.G.IT.B.1	조직 자산(예: 외부적으로 호스팅되는 하드웨어, 소프트웨어, 데이터 및 시스템)의 인벤토리가 유지 관리됩니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의

제어 ID	제어 설명	AWS 구성 규칙	지침
			기본 구성을 쉽게 수행할 수 있습니다.
D1.G.IT.B.1	조직 자산(예: 외부적으로 호스팅되는 하드웨어, 소프트웨어, 데이터 및 시스템)의 인벤토리가 유지 관리됩니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
D1.G.IT.B.1	조직 자산(예: 외부적으로 호스팅되는 하드웨어, 소프트웨어, 데이터 및 시스템)의 인벤토리가 유지 관리됩니다.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
D1.RM.Rm.B.1	기관 내에 정보 보안 및 비즈니스 연속성 위험 관리 기능이 있습니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D1.RM.RA.B.2	위험 평가는 추가 인증 제어가 필요한 인터넷 기반 시스템 및 고위험 거래를 식별합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
D1.RM.RA.B.2	위험 평가는 추가 인증 제어가 필요한 인터넷 기반 시스템 및 고위험 거래를 식별합니다.	annual-risk-assessment-performed (process check)	조직에 대한 연간 위험 평가를 수행합니다. 위험 평가는 식별된 위험 및/또는 취약성이 조직에 영향을 미칠 가능성과 영향을 파악하는 데 도움이 될 수 있습니다.
D1.TC.Tr.B.2	연간 정보 보안 교육에는 인시던트 대응, 현재의 사이버 위협(예: 피싱, 스피어 피싱, 소셜 엔지니어링, 모바일 보안) 및 새로운 문제가 포함됩니다.	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.IS.Is.B.1	정보 보안 위협이 수집되어 해당 내부 직원과 공유됩니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
D2.IS.Is.B.1	정보 보안 위협이 수집되어 해당 내부 직원과 공유됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.IS.Is.B.1	정보 보안 위협이 수집되어 해당 내부 직원과 공유됩니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	cw-loggroup-retent ion-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.1	감사 로그 기록 및 기타 보안 이벤트 로그가 안전한 방식으로 검토 및 보관됩니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
D2.MA.Ma.B.2	컴퓨터 이벤트 로그는 이벤트가 발생한 후 조사에 사용됩니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
D2.MA.Ma.B.2	컴퓨터 이벤트 로그는 이벤트가 발생한 후 조사에 사용됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.2	컴퓨터 이벤트 로그는 이벤트가 발생한 후 조사에 사용됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
D2.MA.Ma.B.2	컴퓨터 이벤트 로그는 이벤트가 발생한 후 조사에 사용됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.2	컴퓨터 이벤트 로그는 이벤트가 발생한 후 조사에 사용됩니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.2	컴퓨터 이벤트 로그는 이벤트가 발생한 후 조사에 사용됩니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
D2.MA.Ma.B.2	컴퓨터 이벤트 로그는 이벤트가 발생한 후 조사에 사용됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.2	컴퓨터 이벤트 로그는 이벤트가 발생한 후 조사에 사용됩니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
D2.MA.Ma.B.2	컴퓨터 이벤트 로그는 이벤트가 발생한 후 조사에 사용됩니다.	redshift-cluster-c onfiguration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDb Encrypted(Config 기본값: TRUE) 및 loggingEnabled(Con fig 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.MA.Ma.B.2	컴퓨터 이벤트 로그는 이벤트가 발생한 후 조사에 사용됩니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.TI.Ti.B.1	기관은 위협에 대한 정보를 제공하는 위협 및 취약성 정보 공유 소스에 속하거나 가입되어 있습니다(예: FS-ISAC, US- CERT).	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.TI.Ti.B.1	기관은 위협에 대한 정보를 제공하는 위협 및 취약성 정보 공유 소스에 속하거나 가입되어 있습니다(예: FS-ISAC, US- CERT).	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
D2.TI.Ti.B.2	위협 정보는 위협과 취약성을 모니터링하는 데 사용됩니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.TI.Ti.B.2	위협 정보는 위협과 취약성을 모니터링하는 데 사용됩니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.TI.Ti.B.2	위협 정보는 위협과 취약성을 모니터링하는 데 사용됩니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.TI.Ti.B.3	위협 정보는 내부 위험 관리 및 통제를 강화하는 데 사용됩니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D2.TI.Ti.B.3	위협 정보는 내부 위험 관리 및 통제를 강화하는 데 사용됩니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
D3.CC.PM.B.1	패치 관리 프로그램이 구현되어 소프트웨어 및 펌웨어 패치가 적시에 적용되도록 합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.CC.PM.B.1	패치 관리 프로그램이 구현되어 소프트웨어 및 펌웨어 패치가 적시에 적용되도록 합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
D3.CC.PM.B.1	패치 관리 프로그램이 구현되어 소프트웨어 및 펌웨어 패치가 적시에 적용되도록 합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.CC.PM.B.1	패치 관리 프로그램이 구현되어 소프트웨어 및 펌웨어 패치가 적시에 적용되도록 합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.CC.PM.B.3	패치 관리 보고서를 검토하여 누락된 보안 패치를 반영합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
D3.CC.PM.B.3	패치 관리 보고서를 검토하여 누락된 보안 패치를 반영합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.CC.PM.B.3	패치 관리 보고서를 검토하여 누락된 보안 패치를 반영합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.CC.PM.B.3	패치 관리 보고서를 검토하여 누락된 보안 패치를 반영합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.1	기관은 환경 전반의 모니터링을 통해 변칙적인 활동을 탐지할 수 있습니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.1	기관은 환경 전반의 모니터링을 통해 변칙적인 활동을 탐지할 수 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.1	기관은 환경 전반의 모니터링을 통해 변칙적인 활동을 탐지할 수 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
D3.DC.An.B.2	변칙적 활동 경고를 생성하는 고객 거래를 모니터링하고 검토합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.2	변칙적 활동 경고를 생성하는 고객 거래를 모니터링하고 검토합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.3	물리적 및/또는 논리적 액세스 로그는 이벤트 이후에 검토됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.3	물리적 및/또는 논리적 액세스 로그는 이벤트 이후에 검토됩니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.3	물리적 및/또는 논리적 액세스 로그는 이벤트 이후에 검토됩니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
D3.DC.An.B.3	물리적 및/또는 논리적 액세스 로그는 이벤트 이후에 검토됩니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.3	물리적 및/또는 논리적 액세스 로그는 이벤트 이후에 검토됩니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
D3.DC.An.B.3	물리적 및/또는 논리적 액세스 로그는 이벤트 이후에 검토됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
D3.DC.An.B.3	물리적 및/또는 논리적 액세스 로그는 이벤트 이후에 검토됩니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.3	물리적 및/또는 논리적 액세스 로그는 이벤트 이후에 검토됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
D3.DC.An.B.3	물리적 및/또는 논리적 액세스 로그는 이벤트 이후에 검토됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.3	물리적 및/또는 논리적 액세스 로그는 이벤트 이후에 검토됩니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
D3.DC.An.B.3	물리적 및/또는 논리적 액세스 로그는 이벤트 이후에 검토됩니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
D3.DC.An.B.4	제3자의 중요 시스템 접근을 모니터링하여 무단 또는 비정상적 활동 여부를 확인합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.An.B.5	승격된 권한은 모니터링됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
D3.DC.An.B.5	승격된 권한은 모니터링됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
D3.DC.Ev.B.1	정상적인 네트워크 활동 기준이 설정됩니다.	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.Ev.B.1	정상적인 네트워크 활동 기준이 설정됩니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
D3.DC.Ev.B.1	정상적인 네트워크 활동 기준이 설정됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
D3.DC.Ev.B.1	정상적인 네트워크 활동 기준이 설정됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.Ev.B.1	정상적인 네트워크 활동 기준이 설정됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
D3.DC.Ev.B.1	정상적인 네트워크 활동 기준이 설정됩니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.Ev.B.1	정상적인 네트워크 활동 기준이 설정됩니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.Ev.B.1	정상적인 네트워크 활동 기준이 설정됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.Ev.B.1	정상적인 네트워크 활동 기준이 설정됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
D3.DC.Ev.B.2	잠재적 공격에 대해 경영진에게 경고하는 메커니즘(예: 안티바이러스 경고, 로그 이벤트 경고)이 마련되어 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.Ev.B.3	무단 사용자, 디바이스, 연결 및 소프트웨어의 존재 여부를 모니터링하는 프로세스가 마련되어 있습니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
D3.DC.Ev.B.3	무단 사용자, 디바이스, 연결 및 소프트웨어의 존재 여부를 모니터링하는 프로세스가 마련되어 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.Ev.B.3	무단 사용자, 디바이스, 연결 및 소프트웨어의 존재 여부를 모니터링하는 프로세스가 마련되어 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.Ev.B.3	무단 사용자, 디바이스, 연결 및 소프트웨어의 존재 여부를 모니터링하는 프로세스가 마련되어 있습니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
D3.DC.Th.B.1	외부 시스템 및 내부 네트워크에 대한 위험 평가에 따라 독립적인 테스트(침투 테스트 및 취약성 검사 포함)가 수행됩니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.DC.Th.B.1	외부 시스템 및 내부 네트워크에 대한 위험 평가에 따라 독립적인 테스트(침투 테스트 및 취약성 검사 포함)가 수행됩니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
D3.DC.Th.B.1	외부 시스템 및 내부 네트워크에 대한 위험 평가에 따라 독립적인 테스트(침투 테스트 및 취약성 검사 포함)가 수행됩니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.1	직무와 최소 권한 원칙에 따라 직원에게 시스템 및 기밀 데이터 액세스 권한이 부여됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
D3.PC.Am.B.1	직무와 최소 권한 원칙에 따라 직원에게 시스템 및 기밀 데이터 액세스 권한이 부여됩니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.1	직무와 최소 권한 원칙에 따라 직원에게 시스템 및 기밀 데이터 액세스 권한이 부여됩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
D3.PC.Am.B.1	직무와 최소 권한 원칙에 따라 직원에게 시스템 및 기밀 데이터 액세스 권한이 부여됩니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.1	직무와 최소 권한 원칙에 따라 직원에게 시스템 및 기밀 데이터 액세스 권한이 부여됩니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
D3.PC.Am.B.1	직무와 최소 권한 원칙에 따라 직원에게 시스템 및 기밀 데이터 액세스 권한이 부여됩니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
D3.PC.Am.B.1	직무와 최소 권한 원칙에 따라 직원에게 시스템 및 기밀 데이터 액세스 권한이 부여됩니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.1	직무와 최소 권한 원칙에 따라 직원에게 시스템 및 기밀 데이터 액세스 권한이 부여됩니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.1	직무와 최소 권한 원칙에 따라 직원에게 시스템 및 기밀 데이터 액세스 권한이 부여됩니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.1	직무와 최소 권한 원칙에 따라 직원에게 시스템 및 기밀 데이터 액세스 권한이 부여됩니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
D3.PC.Am.B.1	직무와 최소 권한 원칙에 따라 직원에게 시스템 및 기밀 데이터 액세스 권한이 부여됩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.10	정보 자산에 대한 무단 액세스 또는 변경을 방지하기 위해 프로덕션 환경과 비프로덕션 환경을 분리합니다. (*해당 기관 또는 기관의 제3자에게 프로덕션 환경이 없는 경우 해당 사항 없음)	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.10	정보 자산에 대한 무단 액세스 또는 변경을 방지하기 위해 프로덕션 환경과 비프로덕션 환경을 분리합니다. (*해당 기관 또는 기관의 제3자에게 프로덕션 환경이 없는 경우 해당 사항 없음)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.10	정보 자산에 대한 무단 액세스 또는 변경을 방지하기 위해 프로덕션 환경과 비프로덕션 환경을 분리합니다. (*해당 기관 또는 기관의 제3자에게 프로덕션 환경이 없는 경우 해당 사항 없음)	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.10	정보 자산에 대한 무단 액세스 또는 변경을 방지하기 위해 프로덕션 환경과 비프로덕션 환경을 분리합니다. (*해당 기관 또는 기관의 제3자에게 프로덕션 환경이 없는 경우 해당 사항 없음)	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
D3.PC.Am.B.12	모든 암호는 보관 및 전송 중에 암호화됩니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.13	공용 또는 신뢰할 수 없는 네트워크(예: 인터넷)를 통해 전송되는 경우 기밀 데이터는 암호화됩니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
D3.PC.Am.B.13	공용 또는 신뢰할 수 없는 네트워크(예: 인터넷)를 통해 전송되는 경우 기밀 데이터는 암호화됩니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.13	공용 또는 신뢰할 수 없는 네트워크(예: 인터넷)를 통해 전송되는 경우 기밀 데이터는 암호화됩니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
D3.PC.Am.B.13	공용 또는 신뢰할 수 없는 네트워크(예: 인터넷)를 통해 전송되는 경우 기밀 데이터는 암호화됩니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
D3.PC.Am.B.13	공용 또는 신뢰할 수 없는 네트워크(예: 인터넷)를 통해 전송되는 경우 기밀 데이터는 암호화됩니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.13	공용 또는 신뢰할 수 없는 네트워크(예: 인터넷)를 통해 전송되는 경우 기밀 데이터는 암호화됩니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
D3.PC.Am.B.13	공용 또는 신뢰할 수 없는 네트워크(예: 인터넷)를 통해 전송되는 경우 기밀 데이터는 암호화됩니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.15	암호화된 연결과 다중 인증을 사용하여 직원, 계약업체 및 제3자가 중요 시스템에 원격으로 액세스합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
D3.PC.Am.B.15	암호화된 연결과 다중 인증을 사용하여 직원, 계약업체 및 제3자가 중요 시스템에 원격으로 액세스합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.15	암호화된 연결과 다중 인증을 사용하여 직원, 계약업체 및 제3자가 중요 시스템에 원격으로 액세스합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.15	암호화된 연결과 다중 인증을 사용하여 직원, 계약업체 및 제3자가 중요 시스템에 원격으로 액세스합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
D3.PC.Am.B.15	암호화된 연결과 다중 인증을 사용하여 직원, 계약업체 및 제3자가 중요 시스템에 원격으로 액세스합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.15	암호화된 연결과 다중 인증을 사용하여 직원, 계약업체 및 제3자가 중요 시스템에 원격으로 액세스합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
D3.PC.Am.B.15	암호화된 연결과 다중 인증을 사용하여 직원, 계약업체 및 제3자가 중요 시스템에 원격으로 액세스합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.16	관리적, 물리적 또는 기술적 통제를 통해 관리자가 아닌 사용자가 무단 소프트웨어를 설치하지 못하도록 합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
D3.PC.Am.B.16	관리적, 물리적 또는 기술적 통제를 통해 관리자가 아닌 사용자가 무단 소프트웨어를 설치하지 못하도록 합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.16	관리적, 물리적 또는 기술적 통제를 통해 관리자가 아닌 사용자가 무단 소프트웨어를 설치하지 못하도록 합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
D3.PC.Am.B.16	관리적, 물리적 또는 기술적 통제를 통해 관리자가 아닌 사용자가 무단 소프트웨어를 설치하지 못하도록 합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.2	직원의 시스템 및 기밀 데이터 액세스가 업무 분리를 제공합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
D3.PC.Am.B.2	직원의 시스템 및 기밀 데이터 액세스가 업무 분리를 제공합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.2	직원의 시스템 및 기밀 데이터 액세스가 업무 분리를 제공합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
D3.PC.Am.B.3	승격된 권한(예: 관리자 권한)은 제한되고 엄격하게 통제됩니다(예: 개인에게 할당, 공유되지 않음, 더 강력한 암호 제어 필요).	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.3	승격된 권한(예: 관리자 권한)은 제한되고 엄격하게 통제됩니다(예: 개인에게 할당, 공유되지 않음, 더 강력한 암호 제어 필요).	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
D3.PC.Am.B.3	승격된 권한(예: 관리자 권한)은 제한되고 엄격하게 통제됩니다(예: 개인에게 할당, 공유되지 않음, 더 강력한 암호 제어 필요).	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.3	승격된 권한(예: 관리자 권한)은 제한되고 엄격하게 통제됩니다(예: 개인에게 할당, 공유되지 않음, 더 강력한 암호 제어 필요).	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
D3.PC.Am.B.3	승격된 권한(예: 관리자 권한)은 제한되고 엄격하게 통제됩니다(예: 개인에게 할당, 공유되지 않음, 더 강력한 암호 제어 필요).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.3	승격된 권한(예: 관리자 권한)은 제한되고 엄격하게 통제됩니다(예: 개인에게 할당, 공유되지 않음, 더 강력한 암호 제어 필요).	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
D3.PC.Am.B.6	시스템, 애플리케이션 및 하드웨어에 액세스하려면 식별 및 인증이 필요하며 관리됩니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.6	시스템, 애플리케이션 및 하드웨어에 액세스하려면 식별 및 인증이 필요하며 관리됩니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
D3.PC.Am.B.6	시스템, 애플리케이션 및 하드웨어에 액세스하려면 식별 및 인증이 필요하며 관리됩니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.6	시스템, 애플리케이션 및 하드웨어에 액세스하려면 식별 및 인증이 필요하며 관리됩니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.6	시스템, 애플리케이션 및 하드웨어에 액세스하려면 식별 및 인증이 필요하며 관리됩니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
D3.PC.Am.B.6	시스템, 애플리케이션 및 하드웨어에 액세스하려면 식별 및 인증이 필요하며 관리됩니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.6	시스템, 애플리케이션 및 하드웨어에 액세스하려면 식별 및 인증이 필요하며 관리됩니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
D3.PC.Am.B.6	시스템, 애플리케이션 및 하드웨어에 액세스하려면 식별 및 인증이 필요하며 관리됩니다.	iam-user-group-membership-check	AWS Identity and Access Managemen t(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.6	시스템, 애플리케이션 및 하드웨어에 액세스하려면 식별 및 인증이 필요하며 관리됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
D3.PC.Am.B.6	시스템, 애플리케이션 및 하드웨어에 액세스하려면 식별 및 인증이 필요하며 관리됩니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.6	시스템, 애플리케이션 및 하드웨어에 액세스하려면 식별 및 인증이 필요하며 관리됩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Am.B.7	액세스 제어에는 암호 복잡성, 암호 시도 및 재사용 제한 등이 포함됩니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
D3.PC.Am.B.8	모든 기본 암호와 불필요한 기본 계정은 시스템 구현 전에 변경됩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
D3.PC.Im.B.1	네트워크 경계 방어 도구(예: 경계 라우터 및 방화벽)가 사용됩니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC 를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.IM.B.2	인터넷이나 외부에서 액세스하는 시스템은 방화벽이나 기타 유사한 디바이스에 의해 보호됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.IM.B.2	인터넷이나 외부에서 액세스하는 시스템은 방화벽이나 기타 유사한 디바이스에 의해 보호됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.IM.B.2	인터넷이나 외부에서 액세스하는 시스템은 방화벽이나 기타 유사한 디바이스에 의해 보호됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.IM.B.2	인터넷이나 외부에서 액세스하는 시스템은 방화벽이나 기타 유사한 디바이스에 의해 보호됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.IM.B.2	인터넷이나 외부에서 액세스하는 시스템은 방화벽이나 기타 유사한 디바이스에 의해 보호됩니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
D3.PC.IM.B.2	인터넷이나 외부에서 액세스하는 시스템은 방화벽이나 기타 유사한 디바이스에 의해 보호됩니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.IM.B.3	모든 포트가 모니터링 됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
D3.PC.IM.B.3	모든 포트가 모니터링 됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
D3.PC.IM.B.3	모든 포트가 모니터링 됩니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.IM.B.3	모든 포트가 모니터링됩니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
D3.PC.IM.B.3	모든 포트가 모니터링됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.IM.B.3	모든 포트가 모니터링됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
D3.PC.Im.B.5	시스템 구성(서버, 데스크톱, 라우터 등)은 업계 표준에 따라 시행됩니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.5	시스템 구성(서버, 데스크톱, 라우터 등)은 업계 표준에 따라 시행됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
D3.PC.Im.B.5	시스템 구성(서버, 데스크톱, 라우터 등)은 업계 표준에 따라 시행됩니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.IM.B.6	비즈니스 목적에 더 이상 필요하지 않은 경우 포트, 기능, 프로토콜 및 서비스가 금지됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.IM.B.6	비즈니스 목적에 더 이상 필요하지 않은 경우 포트, 기능, 프로토콜 및 서비스가 금지됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
D3.PC.IM.B.6	비즈니스 목적에 더 이상 필요하지 않은 경우 포트, 기능, 프로토콜 및 서비스가 금지됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.IM.B.6	비즈니스 목적에 더 이상 필요하지 않은 경우 포트, 기능, 프로토콜 및 서비스가 금지됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.7	시스템 구성(가상 머신 및 하이퍼바이저 포함) 변경에 대한 액세스가 제어되고 모니터링됩니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
D3.PC.Im.B.7	시스템 구성(가상 머신 및 하이퍼바이저 포함) 변경에 대한 액세스가 제어되고 모니터링됩니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.7	시스템 구성(가상 머신 및 하이퍼바이저 포함) 변경에 대한 액세스가 제어되고 모니터링됩니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
D3.PC.Im.B.7	시스템 구성(가상 머신 및 하이퍼바이저 포함) 변경에 대한 액세스가 제어되고 모니터링됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Im.B.7	시스템 구성(가상 머신 및 하이퍼바이저 포함) 변경에 대한 액세스가 제어되고 모니터링됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
D3.PC.Im.B.7	시스템 구성(가상 머신 및 하이퍼바이저 포함) 변경에 대한 액세스가 제어되고 모니터링됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
D3.PC.Im.B.7	시스템 구성(가상 머신 및 하이퍼바이저 포함) 변경에 대한 액세스가 제어되고 모니터링됩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D3.PC.Se.B.1	이 기관에서 일하는 개발자들은 시스템 개발 수명 주기(SDLC) 의 일환으로 업계 표준을 충족하는 보안 프로그램 코딩 관행을 따릅니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
D3.PC.Se.B.1	이 기관에서 일하는 개발자들은 시스템 개발 수명 주기(SDLC) 의 일환으로 업계 표준을 충족하는 보안 프로그램 코딩 관행을 따릅니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D4.C.Co.B.2	기관은 타사 연결이 승인되었는지 확인합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D4.C.Co.B.2	기관은 타사 연결이 승인되었는지 확인합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
D4.C.Co.B.2	기관은 타사 연결이 승인되었는지 확인합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D4.C.Co.B.2	기관은 타사 연결이 승인되었는지 확인합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.1	경고 파라미터는 완화 조치를 유도하는 정보 보안 인시던트를 탐지하기 위해 설정됩니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.1	경고 파라미터는 완화 조치를 유도하는 정보 보안 인시던트를 탐지하기 위해 설정됩니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.1	경고 파라미터는 완화 조치를 유도하는 정보 보안 인시던트를 탐지하기 위해 설정됩니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
D5.DR.De.B.2	시스템 성능 보고서에는 정보 보안 인시던트를 탐지하기 위한 위험 지표로 사용할 수 있는 정보가 포함됩니다.	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.2	시스템 성능 보고서에는 정보 보안 인시던트를 탐지하기 위한 위험 지표로 사용할 수 있는 정보가 포함됩니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.DR.De.B.3	인시던트 대응 프로그램을 탐지, 경고 및 트리거하기 위한 도구와 프로세스가 마련되어 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.ER.Es.B.4	인시던트는 분류, 기록 및 추적됩니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
D5.IR.Pl.B.1	이 기관은 사이버 인시던트에 어떻게 대응하고 대응할 것인지 문서화했습니다.	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
D5.IR.PI.B.6	이 기관은 인시던트 발생 후 업무 연속성, 재해 복구 및 데이터 백업 프로그램을 사용하여 운영을 복구할 계획입니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

템플릿

템플릿은 GitHub: FFIEC 운영 모범 사례에서 확인할 수 있습니다.

독일 C5(Cloud Computing Compliance Criteria Catalog) 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 독일 클라우드 컴퓨팅 규정 준수 기준 카탈로그(C5)와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 독일 C5 제어와 관련이 있습니다. 하나의 독일 C5 제어가 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	AWS 구성 규칙	지침
COS-01	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
COS-01	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
COS-01	waf-regional-rule-not-empty	AWS WAF에 비어 있지 않은 규칙이 있는지 확인합니다. 조건이 없는 규칙에는 의도하지 않은 동작이 발생할 수 있습니다.
COS-01	waf-regional-rulegroup-not-empty	AWS WAF에 비어 있지 않은 규칙 그룹이 있는지 확인합니다. 규칙 그룹이 비어 있으면 의

제어 ID	AWS 구성 규칙	지침
		도하지 않은 동작이 발생할 수 있습니다.
COS-01	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.
COS-01	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
COS-03	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
COS-03	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
COS-03	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
COS-03	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
COS-03	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
COS-03	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
COS-03	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
COS-03	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
COS-03	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
COS-03	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
COS-03	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
COS-03	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
COS-03	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
COS-03	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
COS-03	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
COS-03	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
COS-03	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
COS-03	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
COS-03	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
COS-03	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
COS-03	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
COS-05	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
COS-05	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
COS-05	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
COS-05	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
COS-05	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
COS-05	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
COS-05	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
COS-05	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
COS-05	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
COS-05	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
COS-05	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
COS-05	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
COS-05	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
CRY-02	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CRY-02	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	AWS 구성 규칙	지침
CRY-02	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.
CRY-02	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
CRY-02	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CRY-02	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CRY-02	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
CRY-02	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CRY-02	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CRY-03	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
CRY-03	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
CRY-03	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
CRY-03	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.
CRY-03	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CRY-03	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	AWS 구성 규칙	지침
CRY-03	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CRY-03	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CRY-03	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CRY-03	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
CRY-03	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
CRY-03	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CRY-03	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CRY-03	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
CRY-03	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CRY-03	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
CRY-03	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
CRY-03	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CRY-03	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CRY-03	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
CRY-04	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
DEV-07	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
DEV-07	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	AWS 구성 규칙	지침
DEV-07	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
DEV-07	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
DEV-07	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
DEV-07	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	AWS 구성 규칙	지침
IDM-01	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
IDM-01	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
IDM-01	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
IDM-01	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
IDM-01	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
IDM-01	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	AWS 구성 규칙	지침
IDM-01	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
IDM-01	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
IDM-01	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IDM-01	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IDM-01	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
IDM-01	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
IDM-01	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
IDM-01	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
IDM-01	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
IDM-01	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).
IDM-01	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
IDM-01	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
IDM-01	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.
IDM-01	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

제어 ID	AWS 구성 규칙	지침
IDM-01	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
IDM-01	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	AWS 구성 규칙	지침
IDM-01	rds-instance-iam-authentication-enabled	시스템 및 자산에 대한 액세스를 제어하기 위해 Amazon Relational Database Service(Amazon RDS) 인스턴스에서 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. 이렇게 하면 데이터베이스를 오가는 네트워크 트래픽이 SSL(Secure Sockets Layer)을 통해 암호화됩니다. 인증은 외부에서 관리되므로 사용자 보안 인증 정보를 데이터베이스에 저장할 필요가 없습니다.
IDM-01	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	AWS 구성 규칙	지침
IDM-03	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
IDM-03	secretsmanager-secret-unused	AWS Secrets Manager에 미사용 자격 증명이 있는 경우 자격 증명을 비활성화 및/또는 제거해야 합니다. 최소 권한 원칙을 위반할 수 있습니다. 이 규칙을 사용하면 값을 unusedForDays(Config 기본값: 90)로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
IDM-08	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
CRY-01	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
IDM-09	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
IDM-09	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
IDM-09	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IDM-09	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
OPS-01	clb-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.

제어 ID	AWS 구성 규칙	지침
OPS-01	elbv2-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.
OPS-01	lambda-vpc-multi-az-check	AWS Lambda 함수가 계정의 Virtual Private Cloud(VPC)에 연결되도록 구성된 경우, 최소 두 개의 서로 다른 가용 영역에 AWS Lambda 함수를 배포하여 단일 영역에서 서비스 중단이 발생할 경우 이벤트를 처리할 수 있는 함수인지 확인합니다.
OPS-01	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
OPS-01	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
OPS-01	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
OPS-01	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
OPS-01	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
OPS-02	clb-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.
OPS-02	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
OPS-02	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 강화된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	AWS 구성 규칙	지침
OPS-02	elbv2-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.
OPS-02	lambda-vpc-multi-az-check	AWS Lambda 함수가 계정의 Virtual Private Cloud(VPC)에 연결되도록 구성된 경우, 최소 두 개의 서로 다른 가용 영역에 AWS Lambda 함수를 배포하여 단일 영역에서 서비스 중단이 발생할 경우 이벤트를 처리할 수 있는 함수인지 확인합니다.
OPS-02	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
OPS-02	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
OPS-02	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
OPS-02	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
OPS-02	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
OPS-07	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
OPS-07	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
OPS-07	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
OPS-07	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
OPS-07	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service(OpenSearch Service)의 고가용성과 내결함성을 위해서는 최소한 3개 이상의 데이터 노드가 필요합니다. 3개 이상의 데이터 노드가 포함된 OpenSearch Service 도메인을 배포하면 노드에 장애가 발생하더라도 클러스터 운영이 보장됩니다.

제어 ID	AWS 구성 규칙	지침
OPS-07	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.
OPS-07	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
OPS-07	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
OPS-07	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
OPS-07	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
OPS-07	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
OPS-07	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
OPS-07	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
OPS-07	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
OPS-07	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
OPS-12	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	AWS 구성 규칙	지침
OPS-12	s3-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
OPS-13	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
OPS-13	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
OPS-13	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
OPS-14	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrai l이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	AWS 구성 규칙	지침
OPS-14	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
OPS-14	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
OPS-14	s3-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
OPS-15	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
OPS-15	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
OPS-15	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
OPS-15	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
OPS-15	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
OPS-15	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
OPS-15	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
OPS-15	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
OPS-15	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.
OPS-15	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
OPS-15	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
OPS-15	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
OPS-15	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
OPS-15	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
OPS-15	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail 에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
OPS-15	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
OPS-22	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository(ECR) 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.

제어 ID	AWS 구성 규칙	지침
PSS-05	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
PSS-05	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
PSS-05	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
PSS-05	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
PSS-07	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

템플릿

템플릿은 GitHub: 독일 C5(Cloud Computing Compliance Criteria Catalog)에서 확인할 수 있습니다.

Gramm Leach Bliley 법(GLBA) 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계

되지 않았습니다. 귀하는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Gramm Leach Bliley 법(GLBA)과 AWS 관리형 Config 규칙 간의 샘플 매핑입니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 GLBA 제어와 관련이 있습니다. GLBA 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	련된 적절한 표준을 수립해야 합니다.		Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립해야 합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	codebuild-project-s3-logs-encrypted	저장 시 민감한 데이터를 보호하려면 Amazon S3에 저장된 your AWS CodeBuild 로그에 대해 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
GLBA-SEC.501(b)(1)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 고객 레코드와 정보의 보안과 기밀을 보장해야 합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(2)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (2) 이러한 레코드의 보안이나 무결성에 대해 예상되는 위협 또는 위험을 차단해야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(2)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (2) 이러한 레코드의 보안이나 무결성에 대해 예상되는 위협 또는 위험을 차단해야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
GLBA-SEC.501(b)(3)	(a) 항의 정책에 따라, 섹션 505(a)에 기술된 각 기관 또는 당국은 관할 대상 금융 기관에 대해 행정적, 기술적, 물리적 보호 조치와 관련된 적절한 표준을 수립하여 (3) 이러한 레코드 또는 정보에 대한 무단 액세스 또는 사용을 차단해야 합니다. 고객에게 상당한 악영향 또는 불편을 초래할 수 있기 때문입니다.	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

템플릿

템플릿은 GitHub: Gramm Leach Bliley 법(GLBA) 운영 모범 사례에서 확인할 수 있습니다.

GxP EU Annex 11 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 GxP EU 부속서 11과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 GxP EU 부속서 11 제어와 관련이 있습니다. GxP EU Annex 11 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1. 위험 관리	위험 관리는 환자 안전, 데이터 무결성 및 제품 품질을 고려하여 컴퓨터 시스템의 수명 주기 전반에 걸쳐 적용되어야 합니다. 위험 관리 시스템의 일환으로 검증 및 데이터 무결성 제어 범위에 대한 결정은 컴퓨터 시스템의 정당하고 문서화된 위험 평가를 기반으로 해야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
1. 위험 관리	위험 관리는 환자 안전, 데이터 무결성 및 제품 품질을 고려하여 컴퓨터 시스템의 수명 주기 전반에 걸쳐 적용되어야 합니다. 위험 관리 시스템의 일환으로 검증 및 데이터 무결성 제어 범위에 대한 결정은 컴퓨터 시스템의 정당하고 문서화된 위험 평가를 기반으로 해야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS

제어 ID	제어 설명	AWS 구성 규칙	지침
			Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
4.2. 검증 - 문서 변경 관리	검증 문서에는 변경 관리 기록(해당하는 경우)과 검증 프로세스 중에 관찰된 편차에 대한 보고서가 포함되어야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.3. 검증 - 인벤토리	모든 관련 시스템 및 해당 GMP 기능(인벤토리)의 최신 목록이 있어야 합니다. 중요 시스템의 경우 물리적 및 논리적 배열, 데이터 흐름 및 다른 시스템 또는 프로세스와의 인터페이스, 하드웨어 및 소프트웨어 사전 요구 사항, 보안 조치를 자세히 설명하는 최신 시스템 설명이 제공되어야 합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.3. 검증 - 인벤토리	모든 관련 시스템 및 해당 GMP 기능(인벤토리)의 최신 목록이 있어야 합니다. 중요 시스템의 경우 물리적 및 논리적 배열, 데이터 흐름 및 다른 시스템 또는 프로세스와의 인터페이스, 하드웨어 및 소프트웨어 사전 요구 사항, 보안 조치를 자세히 설명하는 최신 시스템 설명이 제공되어야 합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
4.3. 검증 - 인벤토리	모든 관련 시스템 및 해당 GMP 기능(인벤토리)의 최신 목록이 있어야 합니다. 중요 시스템의 경우 물리적 및 논리적 배열, 데이터 흐름 및 다른 시스템 또는 프로세스와의 인터페이스, 하드웨어 및 소프트웨어 사전 요구 사항, 보안 조치를 자세히 설명하는 최신 시스템 설명이 제공되어야 합니다.	ec2-security-group-attached-to-eni-periodic	자산 인벤토리를 관리하는 데 도움이 되도록 이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 Elastic Network 인터페이스 중 어디에 연결되어 있는지 확인합니다. 보안 그룹이 이러한 리소스 유형에 연결되어 있지 않은 경우, 사용되지 않아 더 이상 필요하지 않을 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.3. 검증 - 인벤토리	모든 관련 시스템 및 해당 GMP 기능(인벤토리)의 최신 목록이 있어야 합니다. 중요 시스템의 경우 물리적 및 논리적 배열, 데이터 흐름 및 다른 시스템 또는 프로세스와의 인터페이스, 하드웨어 및 소프트웨어 사전 요구 사항, 보안 조치를 자세히 설명하는 최신 시스템 설명이 제공되어야 합니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
4.3. 검증 - 인벤토리	모든 관련 시스템 및 해당 GMP 기능(인벤토리)의 최신 목록이 있어야 합니다. 중요 시스템의 경우 물리적 및 논리적 배열, 데이터 흐름 및 다른 시스템 또는 프로세스와의 인터페이스, 하드웨어 및 소프트웨어 사전 요구 사항, 보안 조치를 자세히 설명하는 최신 시스템 설명이 제공되어야 합니다.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.3. 검증 - 인벤토리	모든 관련 시스템 및 해당 GMP 기능(인벤토리)의 최신 목록이 있어야 합니다. 중요 시스템의 경우 물리적 및 논리적 배열, 데이터 흐름 및 다른 시스템 또는 프로세스와의 인터페이스, 하드웨어 및 소프트웨어 사전 요구 사항, 보안 조치를 자세히 설명하는 최신 시스템 설명이 제공되어야 합니다.	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.8. 검증 - 데이터 전송	데이터가 다른 데이터 형식이나 시스템으로 전송되는 경우, 검증에는 마이그레이션 프로세스 중에 데이터의 가치 및/또는 의미가 변경되지 않았는지 확인하는 작업이 포함되어야 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	EBS-in-Backup-plan-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 데이터	다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터 시스템에는 위험을 최소화하기 위해 데이터를 정확하고 안전하게 입력하고 처리하는 데 필요한 적절한 내장 검사 기능이 포함되어야 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	EBS-in-Backup-plan-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1. 데이터 스토리지 - 손상 방지	데이터는 손상되지 않도록 물리적 및 전자적 수단을 통해 보호되어야 합니다. 저장된 데이터의 접근성, 가독성 및 정확성을 검사해야 합니다. 보관 기간 내내 데이터에 대한 액세스가 보장되어야 합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	EBS-in-Backup-plan-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2. 데이터 스토리지 - 백업	모든 관련 데이터를 정기적으로 백업해야 합니다. 검증 과정에서 백업 데이터의 무결성과 정확성, 데이터 복원 기능을 확인하고 주기적으로 모니터링해야 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
9. 감사 추적	위험 평가를 기반으로 모든 GMP 관련 변경 및 삭제 기록(시스템에서 생성한 “감사 추적”)을 시스템에 생성하는 것을 고려해야 합니다. GMP 관련 데이터를 변경하거나 삭제하려면 이유를 문서화해야 합니다. 감사 추적은 이용 가능하고 일반적으로 이해하기 쉬운 형식으로 변환 가능하며 정기적으로 검토할 수 있어야 합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10. 변경 및 구성 관리	시스템 구성을 포함하여 컴퓨터 시스템에 대한 모든 변경은 정의된 절차에 따라 통제된 방식으로만 이루어져야 합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
10. 변경 및 구성 관리	시스템 구성을 포함하여 컴퓨터 시스템에 대한 모든 변경은 정의된 절차에 따라 통제된 방식으로만 이루어져야 합니다.	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10. 변경 및 구성 관리	시스템 구성을 포함하여 컴퓨터 시스템에 대한 모든 변경은 정의된 절차에 따라 통제된 방식으로만 이루어져야 합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
11. 정기 평가	컴퓨터 시스템을 정기적으로 평가하여 유효한 상태를 유지하고 GMP를 준수하는지 확인해야 합니다. 이러한 평가에는 적절한 경우 현재 기능 범위, 편차 기록, 인시던트, 문제, 업그레이드 기록, 성능, 안정성, 보안 및 검증 상태 보고서가 포함되어야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	codebuild-project-environment-privileged-check	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있지 않은지 확인합니다. Docker API와 컨테이너의 기본 하드웨어에 대해 의도하지 않은 액세스를 방지하려면 이 설정을 비활성화해야 합니다.
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	ec2 인스턴스 프로필 첨부	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	rds-instance-iam-authentication-enabled	시스템 및 자산에 대한 액세스를 제어하기 위해 Amazon Relational Database Service(Amazon RDS) 인스턴스에서 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. 이렇게 하면 데이터베이스를 오가는 네트워크 트래픽이 SSL(Secure Sockets Layer)을 통해 암호화됩니다. 인증은 외부에서 관리되므로 사용자 보안 인증 정보를 데이터베이스에 저장할 필요가 없습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.1. 보안 - 권한을 부여받은 사람	승인된 사람만 컴퓨터 시스템에 접근하도록 제한할 수 있는 물리적 및/또는 논리적 통제를 마련해야 합니다. 시스템에 대한 무단 침입을 방지하는 적절한 방법에는 키, 출입 카드, 암호가 포함된 개인 코드, 생체 인식 사용, 컴퓨터 장비 및 데이터 저장 영역에 대한 접근 제한 등이 포함될 수 있습니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
12.3. 보안 - 권한 부여 감사 추적	액세스 권한 생성, 변경 및 취소를 기록해야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.4. 보안 - 감사 추적	데이터 및 문서 관리 시스템은 날짜 및 시간을 포함하여 데이터를 입력, 변경, 확인 또는 삭제하는 운영자의 신원을 기록하도록 설계되어야 합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13. 인시던트 관리	시스템 장애 및 데이터 오류뿐만 아니라 모든 인시던트를 보고하고 평가해야 합니다. 중대한 인시던트의 근본 원인을 파악하고 시정 및 예방 조치의 기초로 삼아야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13. 인시던트 관리	시스템 장애 및 데이터 오류뿐만 아니라 모든 인시던트를 보고하고 평가해야 합니다. 중대한 인시던트의 근본 원인을 파악하고 시정 및 예방 조치의 기초로 삼아야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	elbv2-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	lambda-vpc-multi-az-check	AWS Lambda 함수가 계정의 Virtual Private Cloud(VPC)에 연결되도록 구성된 경우, 최소 두 개의 서로 다른 가용 영역에 AWS Lambda 함수를 배포하여 단일 영역에서 서비스 중단이 발생할 경우 이벤트를 처리할 수 있는 함수인지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service(OpenSearch Service)의 고가용성과 내결함성을 위해서는 최소한 3개 이상의 데이터 노드가 필요합니다. 3개 이상의 데이터 노드가 포함된 OpenSearch Service 도메인을 배포하면 노드에 장애가 발생하더라도 클러스터 운영이 보장됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS) 클러스터에는 저장된 데이터의 가용성을 지원하기 위해 다중 AZ 복제가 활성화되어 있어야 합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
16. 비즈니스 연속성	중요한 프로세스를 지원하는 컴퓨터 시스템을 사용하려면 시스템 장애 발생 시 해당 프로세스에 대한 지원이 지속되도록 보장할 수 있는 조항을 마련해야 합니다(예: 수동 또는 대체 시스템). 대체 조치를 적용하는 데 필요한 시간은 위험을 기준으로 하고 특정 시스템 및 해당 시스템이 지원하는 비즈니스 프로세스에 적합해야 합니다. 이러한 조치를 적절히 문서화하고 테스트해야 합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
17. 보관	데이터가 보관될 수 있습니다. 이 데이터의 접근성, 가독성 및 무결성을 검사해야 합니다. 시스템(예: 컴퓨터 장비 또는 프로그램)에 관련 변경이 필요한 경우 데이터 검색 기능을 보장하고 테스트해야 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

템플릿

템플릿은 GitHub: GxP EU Annex 11 운영 모범 사례에서 확인할 수 있습니다.

HIPAA 보안 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 HIPAA(Health Insurance Portability and Accountability Act)와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 HIPAA 제어와 관련이 있습니다. HIPAA 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 적합성 팩은 Payment Card Industry Qualified Security Assessors(QSAs), HITRUST Certified Common Security Framework Practitioners(CCSFPs AWS) 및 다양한 산업 프레임워크에 대한 지

침과 평가를 제공하도록 인증된 규정 준수 전문가로 구성된 팀인 AWS Security Assurance Services LLC(AWS SAS)에서 검증되었습니다.SAS 전문가는 고객이 HIPAA의 하위 집합에 맞게이 적합성 팩을 설계했습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(A)	(A) 위험 분석(필수). 피보험자가 보유한 전자적으로 보호된 의료 정보의 기밀성, 무결성 및 가용성에 대한 잠재적 위험 및 취약성을 정확하고 철저하게 평가합니다.	annual-risk-assessment-performed(프로세스 확인)	조직에 대한 연간 위험 평가를 수행합니다. 위험 평가는 식별된 위험 및/또는 취약성이 조직에 영향을 미칠 가능성과 영향을 파악하는 데 도움이 될 수 있습니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거

제어 ID	제어 설명	AWS 구성 규칙	지침
			나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(1)(ii)(B)	(B) 위험 관리(필수). 섹션 164.306(a)을 준수할 수 있도록 위험과 취약성을 합리적이고 적절한 수준으로 줄일 수 있는 충분한 보안 조치를 구현합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(i)	(3)(i) 표준: 인력 보안. 이 섹션의 (a)(4)항에 따라 모든 직원이 전자적으로 보호된 의료 정보에 적절하게 접근할 수 있도록 하고, 이 섹션의 (a)(4)항에 따라 접근 권한이 없는 근로자가 전자적으로 보호된 의료 정보에 접근하지 못하도록 하는 정책 및 절차를 구현합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	iam-inline-policy-blocked-blocked-KMS-action	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(A)	(A) 권한 부여 및/또는 감독(주소 지정 가능). 전자적으로 보호된 의료 정보를 다루는 작업자 또는 해당 정보에 액세스할 수 있는 위치에 있는 직원에 대한 권한 부여 및/또는 감독 절차를 구현합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(B)	(B) 인력 허가 절차(주소 지정 가능). 직원이 전자적으로 보호된 의료 정보에 액세스하는 것이 적절한지 판단하는 절차를 구현합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(B)	(B) 인력 허가 절차(주소 지정 가능). 직원이 전자적으로 보호된 의료 정보에 액세스하는 것이 적절한지 판단하는 절차를 구현합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
164.308(a)(3)(ii)(B)	(B) 인력 허가 절차(주소 지정 가능). 직원이 전자적으로 보호된 의료 정보에 액세스하는 것이 적절한지 판단하는 절차를 구현합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(B)	(B) 인력 허가 절차(주소 지정 가능). 직원이 전자적으로 보호된 의료 정보에 액세스하는 것이 적절한지 판단하는 절차를 구현합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
164.308(a)(3)(ii)(B)	(B) 인력 허가 절차(주소 지정 가능). 직원이 전자적으로 보호된 의료 정보에 액세스하는 것이 적절한지 판단하는 절차를 구현합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(B)	(B) 인력 허가 절차(주소 지정 가능). 직원이 전자적으로 보호된 의료 정보에 액세스하는 것이 적절한지 판단하는 절차를 구현합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(B)	(B) 인력 허가 절차(주소 지정 가능). 직원이 전자적으로 보호된 의료 정보에 액세스하는 것이 적절한지 판단하는 절차를 구현합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
164.308(a)(3)(ii)(B)	(B) 인력 허가 절차(주소 지정 가능). 직원이 전자적으로 보호된 의료 정보에 액세스하는 것이 적절한지 판단하는 절차를 구현합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(B)	(B) 인력 허가 절차(주소 지정 가능). 직원이 전자적으로 보호된 의료 정보에 액세스하는 것이 적절한지 판단하는 절차를 구현합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
164.308(a)(3)(ii)(B)	(B) 인력 허가 절차(주소 지정 가능). 직원이 전자적으로 보호된 의료 정보에 액세스하는 것이 적절한지 판단하는 절차를 구현합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(B)	(B) 인력 허가 절차(주소 지정 가능). 직원이 전자적으로 보호된 의료 정보에 액세스하는 것이 적절한지 판단하는 절차를 구현합니다.	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(3)(ii)(C)	(C) 해지 절차(주소 지정 가능). 직원의 고용이 종료될 때 또는 이 섹션의 (a)(3)(ii)(B)항에 명시된 결정에 따라 필요한 경우 전자적으로 보호된 의료 정보에 대한 접근을 종료하는 절차를 구현합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(i)	(4)(i) 표준: 정보 액세스 관리. 이 부분의 하위 파트 E의 해당 요구사항과 일치하는 전자적으로 보호된 건강 정보에 대한 액세스를 승인하기 위한 정책 및 절차를 구현합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(i)	(4)(i) 표준: 정보 액세스 관리. 이 부분의 하위 파트 E의 해당 요구 사항과 일치하는 전자적으로 보호된 건강 정보에 대한 액세스를 승인하기 위한 정책 및 절차를 구현합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
164.308(a)(4)(i)	(4)(i) 표준: 정보 액세스 관리. 이 부분의 하위 파트 E의 해당 요구 사항과 일치하는 전자적으로 보호된 건강 정보에 대한 액세스를 승인하기 위한 정책 및 절차를 구현합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(i)	(4)(i) 표준: 정보 액세스 관리. 이 부분의 하위 파트 E의 해당 요구사항과 일치하는 전자적으로 보호된 건강 정보에 대한 액세스를 승인하기 위한 정책 및 절차를 구현합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
164.308(a)(4)(i)	(4)(i) 표준: 정보 액세스 관리. 이 부분의 하위 파트 E의 해당 요구사항과 일치하는 전자적으로 보호된 건강 정보에 대한 액세스를 승인하기 위한 정책 및 절차를 구현합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(i)	(4)(i) 표준: 정보 액세스 관리. 이 부분의 하위 파트 E의 해당 요구 사항과 일치하는 전자적으로 보호된 건강 정보에 대한 액세스를 승인하기 위한 정책 및 절차를 구현합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(i)	(4)(i) 표준: 정보 액세스 관리. 이 부분의 하위 파트 E의 해당 요구사항과 일치하는 전자적으로 보호된 건강 정보에 대한 액세스를 승인하기 위한 정책 및 절차를 구현합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
164.308(a)(4)(i)	(4)(i) 표준: 정보 액세스 관리. 이 부분의 하위 파트 E의 해당 요구사항과 일치하는 전자적으로 보호된 건강 정보에 대한 액세스를 승인하기 위한 정책 및 절차를 구현합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(i)	(4)(i) 표준: 정보 액세스 관리. 이 부분의 하위 파트 E의 해당 요구 사항과 일치하는 전자적으로 보호된 건강 정보에 대한 액세스를 승인하기 위한 정책 및 절차를 구현합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
164.308(a)(4)(i)	(4)(i) 표준: 정보 액세스 관리. 이 부분의 하위 파트 E의 해당 요구 사항과 일치하는 전자적으로 보호된 건강 정보에 대한 액세스를 승인하기 위한 정책 및 절차를 구현합니다.	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	iam-inline-policy-blocked-blocked-KMS-action	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(A)	(A) 의료 정보 센터 기능 격리(필수). 의료 정보 센터가 대규모 조직의 일부인 경우 정보 센터는 정보 센터의 전자적으로 보호된 건강 정보가 대규모 조직의 무단 액세스로부터 보호되는 것을 방지하는 정책과 절차를 시행해야 합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
164.308(a)(4)(ii)(B)	(B) 액세스 권한 부여(주소 지정 가능). 예를 들어 워크스테이션, 트랜잭션, 프로그램, 프로세스 또는 기타 메커니즘에 대한 액세스를 통해 전자적으로 보호된 의료 정보에 대한 액세스 권한을 부여하는 정책 및 절차를 구현합니다.	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(4)(ii)(C)	(C) 액세스 설정 및 수정(주소 지정 가능). 기관의 액세스 권한 부여 정책을 기반으로 워크스테이션, 트랜잭션, 프로그램 또는 프로세스에 대한 사용자의 액세스 권한을 수립, 문서화, 검토 및 수정하는 정책 및 절차를 구현합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
164.308(a)(5)(ii)(A)	(A) 보안 알림(주소 지정 가능). 정기 보안 업데이트.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(5)(ii)(A)	(A) 보안 알림(주소 지정 가능). 정기 보안 업데이트.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(5)(ii)(A)	(A) 보안 알림(주소 지정 가능). 정기 보안 업데이트.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(5)(ii)(A)	(A) 보안 알림(주소 지정 가능). 정기 보안 업데이트.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
164.308(a)(5)(ii)(B)	(B) 악성 소프트웨어로부터 보호(주소 지정 가능). 악성 소프트웨어로부터 보호, 탐지 및 신고하기 위한 절차.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(5)(ii)(B)	(B) 악성 소프트웨어로부터 보호(주소 지정 가능). 악성 소프트웨어로부터 보호, 탐지 및 신고하기 위한 절차.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
164.308(a)(5)(ii)(B)	(B) 악성 소프트웨어로부터 보호(주소 지정 가능). 악성 소프트웨어로부터 보호, 탐지 및 신고하기 위한 절차.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(5)(ii)(C)	(C) 로그인 모니터링 (주소 지정 가능). 로그인 시도를 모니터링하고 불일치를 보고하는 절차.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
164.308(a)(5)(ii)(C)	(C) 로그인 모니터링 (주소 지정 가능). 로그인 시도를 모니터링하고 불일치를 보고하는 절차.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(5)(ii)(C)	(C) 로그인 모니터링 (주소 지정 가능). 로그인 시도를 모니터링하고 불일치를 보고하는 절차.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(5)(ii)(D)	(D) 암호 관리(주소 지정 가능). 암호 생성, 변경 및 보호 절차.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
164.308(a)(6)(i)	(6)(i) 표준: 보안 인시던트 절차. 보안 인시던트를 해결하기 위한 정책 및 절차를 구현합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(6)(ii)	(ii) 구현 사양: 대응 및 보고(필수). 의심되거나 알려진 보안 인시던트를 식별하여 이에 대응하고, 해당 대상에게 알려진 보안 인시던트의 유해한 영향을 실행 가능한 범위 내에서 완화하고, 보안 인시던트 및 그 결과를 문서화합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(i)	(7)(i) 표준: 비상 계획. 전자적으로 보호되는 의료 정보가 포함된 시스템을 손상하는 비상 상황 또는 기타 상황(예: 화재, 기물 파손, 시스템 장애, 자연 재해)에 대응하기 위한 정책 및 절차를 수립(및 필요에 따라 구현)합니다.	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획(필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획 (필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획 (필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획(필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획(필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획 (필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획 (필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획 (필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획 (필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획 (필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획 (필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(A)	(A) 데이터 백업 계획 (필수). 전자적으로 보호되는 의료 정보의 검색 가능한 정확한 사본을 만들고 유지하기 위한 절차를 수립하고 구현합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(B)	(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 수립(및 필요에 따라 구현)합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
164.308(a)(7)(ii)(B)	(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 수립(및 필요에 따라 구현)합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(B)	(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 수립(및 필요에 따라 구현)합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
164.308(a)(7)(ii)(B)	(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 수립(및 필요에 따라 구현)합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(B)	(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 수립(및 필요에 따라 구현)합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
164.308(a)(7)(ii)(B)	(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 수립(및 필요에 따라 구현)합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(B)	(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 수립(및 필요에 따라 구현)합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
164.308(a)(7)(ii)(B)	(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 수립(및 필요에 따라 구현)합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(B)	(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 수립(및 필요에 따라 구현)합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
164.308(a)(7)(ii)(B)	(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 수립(및 필요에 따라 구현)합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(B)	(B) 재해 복구 계획(필수). 데이터 손실을 복원하기 위한 절차를 수립(및 필요에 따라 구현)합니다.	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
164.308(a)(7)(ii)(C)	(C) 비상 모드 운영 계획(필수). 비상 모드에서 운영하는 동안 전자적으로 보호되는 의료 정보의 보안을 보호하기 위한 중요한 비즈니스 프로세스를 지속할 수 있는 절차를 수립(및 필요에 따라 구현)합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(C)	(C) 비상 모드 운영 계획(필수). 비상 모드에서 운영하는 동안 전자적으로 보호되는 의료 정보의 보안을 보호하기 위한 중요한 비즈니스 프로세스를 지속할 수 있는 절차를 수립(및 필요에 따라 구현)합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
164.308(a)(7)(ii)(C)	(C) 비상 모드 운영 계획(필수). 비상 모드에서 운영하는 동안 전자적으로 보호되는 의료 정보의 보안을 보호하기 위한 중요한 비즈니스 프로세스를 지속할 수 있는 절차를 수립(및 필요에 따라 구현)합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(C)	(C) 비상 모드 운영 계획(필수). 비상 모드에서 운영하는 동안 전자적으로 보호되는 의료 정보의 보안을 보호하기 위한 중요한 비즈니스 프로세스를 지속할 수 있는 절차를 수립(및 필요에 따라 구현)합니다.	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(C)	(C) 비상 모드 운영 계획(필수). 비상 모드에서 운영하는 동안 전자적으로 보호되는 의료 정보의 보안을 보호하기 위한 중요한 비즈니스 프로세스를 지속할 수 있는 절차를 수립(및 필요에 따라 구현)합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(7)(ii)(C)	(C) 비상 모드 운영 계획(필수). 비상 모드에서 운영하는 동안 전자적으로 보호되는 의료 정보의 보안을 보호하기 위한 중요한 비즈니스 프로세스를 지속할 수 있는 절차를 수립(및 필요에 따라 구현)합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(8)	(8) 표준: 평가. 처음에는 이 규칙에 따라 구현된 표준을 기반으로 하고 이후에는 전자적으로 보호되는 의료 정보의 보안에 영향을 미치는 환경 또는 운영상의 변화에 대응하여 정기적인 기술 및 비기술적 평가를 수행함으로써 기관의 보안 정책 및 절차가 이 하위 파트의 요구 사항을 충족하는 정도를 결정합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.308(a)(8)	(8) 표준: 평가. 처음에는 이 규칙에 따라 구현된 표준을 기반으로 하고 이후에는 전자적으로 보호되는 의료 정보의 보안에 영향을 미치는 환경 또는 운영상의 변화에 대응하여 정기적인 기술 및 비기술적 평가를 수행함으로써 기관의 보안 정책 및 절차가 이 하위 파트의 요구 사항을 충족하는 정도를 결정합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(1)	(a) (1) 표준: 액세스 제어. 164.308(a)(4)에 명시된 대로 접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 접근을 허용하기 위해, 전자적으로 보호되는 의료 정보를 유지하는 전자 정보 시스템에 대한 기술 정책 및 절차를 구현합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(i)	(2) 구현 사양: (i) 고유한 사용자 식별(필수). 사용자 신원을 식별하고 추적하기 위해 고유한 이름 및/또는 번호를 할당합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
164.312(a)(2)(ii)	(ii) 비상 액세스 절차(필수). 응급 상황 중에 필요한 전자적으로 보호되는 의료 정보를 확보하기 위한 절차를 수립(및 필요에 따라 시행)합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(a)(2)(iv)	(iv) 암호화 및 암호 해독(주소 지정 가능). 전자적으로 보호되는 의료 정보를 암호화하고 해독하는 메커니즘을 구현합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	s3-event-notifications-enabled	Amazon S3 이벤트 알림은 버킷 객체가 우발적이거나 의도적으로 수정된 경우 관련 담당자에게 알릴 수 있습니다. 알림의 예로는 새 객체 생성, 객체 제거, 객체 복원, 분실 및 복제된 객체 등이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(b)	(b) 표준: 감사 통제. 전자적으로 보호되는 의료 정보를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검사하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
164.312(c)(1)	(c)(1) 표준: 무결성. 전자적으로 보호된 의료 정보가 부적절하게 변경 또는 파괴되지 않도록 보호하기 위한 정책 및 절차를 구현합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(c)(1)	(c)(1) 표준: 무결성. 전자적으로 보호된 의료 정보가 부적절하게 변경 또는 파괴되지 않도록 보호하기 위한 정책 및 절차를 구현합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(c)(1)	(c)(1) 표준: 무결성. 전자적으로 보호된 의료 정보가 부적절하게 변경 또는 파괴되지 않도록 보호하기 위한 정책 및 절차를 구현합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
164.312(c)(1)	(c)(1) 표준: 무결성. 전자적으로 보호된 의료 정보가 부적절하게 변경 또는 파괴되지 않도록 보호하기 위한 정책 및 절차를 구현합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(c)(1)	(c)(1) 표준: 무결성. 전자적으로 보호된 의료 정보가 부적절하게 변경 또는 파괴되지 않도록 보호하기 위한 정책 및 절차를 구현합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(c)(2)	(2) 구현 사양: 전자적으로 보호되는 의료 정보를 인증하는 메커니즘(주소 지정 가능). 전자적으로 보호되는 의료 정보가 무단으로 변경 또는 파괴되지 않았음을 확인하는 전자 메커니즘을 구현합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
164.312(c)(2)	(2) 구현 사양: 전자적으로 보호되는 의료 정보를 인증하는 메커니즘(주소 지정 가능). 전자적으로 보호되는 의료 정보가 무단으로 변경 또는 파괴되지 않았음을 확인하는 전자 메커니즘을 구현합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(c)(2)	(2) 구현 사양: 전자적으로 보호되는 의료 정보를 인증하는 메커니즘(주소 지정 가능). 전자적으로 보호되는 의료 정보가 무단으로 변경 또는 파괴되지 않았음을 확인하는 전자 메커니즘을 구현합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(c)(2)	(2) 구현 사양: 전자적으로 보호되는 의료 정보를 인증하는 메커니즘(주소 지정 가능). 전자적으로 보호되는 의료 정보가 무단으로 변경 또는 파괴되지 않았음을 확인하는 전자 메커니즘을 구현합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(c)(2)	(2) 구현 사양: 전자적으로 보호되는 의료 정보를 인증하는 메커니즘(주소 지정 가능). 전자적으로 보호되는 의료 정보가 무단으로 변경 또는 파괴되지 않았음을 확인하는 전자 메커니즘을 구현합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(d)	(d) 표준: 개인 또는 법인 인증. 전자적으로 보호되는 의료 정보에 대한 접근을 원하는 개인 또는 법인이 클레임된 당사자인지 확인하는 절차를 구현합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
164.312(d)	(d) 표준: 개인 또는 법인 인증. 전자적으로 보호되는 의료 정보에 대한 접근을 원하는 개인 또는 법인이 클레임된 당사자인지 확인하는 절차를 구현합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(d)	(d) 표준: 개인 또는 법인 인증. 전자적으로 보호되는 의료 정보에 대한 접근을 원하는 개인 또는 법인이 클레임된 당사자인지 확인하는 절차를 구현합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(d)	(d) 표준: 개인 또는 법인 인증. 전자적으로 보호되는 의료 정보에 대한 접근을 원하는 개인 또는 법인이 클레임된 당사자인지 확인하는 절차를 구현합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
164.312(d)	(d) 표준: 개인 또는 법인 인증. 전자적으로 보호되는 의료 정보에 대한 접근을 원하는 개인 또는 법인이 클레임된 당사자인지 확인하는 절차를 구현합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(1)	(e) (1) 표준: 전송 보안. 전자 통신 네트워크를 통해 전송되는 전자적으로 보호되는 의료 정보에 대한 무단 액세스를 방지하기 위한 기술적 보안 조치를 구현합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(i)	(i) 무결성 제어(주소 지정 가능). 전자적으로 전송된 전자적으로 보호되는 의료 정보가 폐기될 때까지 탐지 없이 부적절하게 수정되지 않도록 보안 조치를 취합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(i)	(i) 무결성 제어(주소 지정 가능). 전자적으로 전송된 전자적으로 보호되는 의료 정보가 폐기될 때까지 탐지 없이 부적절하게 수정되지 않도록 보안 조치를 취합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
164.312(e)(2)(i)	(i) 무결성 제어(주소 지정 가능). 전자적으로 전송된 전자적으로 보호되는 의료 정보가 폐기될 때까지 탐지 없이 부적절하게 수정되지 않도록 보안 조치를 취합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(i)	(i) 무결성 제어(주소 지정 가능). 전자적으로 전송된 전자적으로 보호되는 의료 정보가 폐기될 때까지 탐지 없이 부적절하게 수정되지 않도록 보안 조치를 취합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(i)	(i) 무결성 제어(주소 지정 가능). 전자적으로 전송된 전자적으로 보호되는 의료 정보가 폐기될 때까지 탐지 없이 부적절하게 수정되지 않도록 보안 조치를 취합니다.	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(i)	(i) 무결성 제어(주소 지정 가능). 전자적으로 전송된 전자적으로 보호되는 의료 정보가 폐기될 때까지 탐지 없이 부적절하게 수정되지 않도록 보안 조치를 취합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(i)	(i) 무결성 제어(주소 지정 가능). 전자적으로 전송된 전자적으로 보호되는 의료 정보가 폐기될 때까지 탐지 없이 부적절하게 수정되지 않도록 보안 조치를 취합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(i)	(i) 무결성 제어(주소 지정 가능). 전자적으로 전송된 전자적으로 보호되는 의료 정보가 폐기될 때까지 탐지 없이 부적절하게 수정되지 않도록 보안 조치를 취합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(i)	(i) 무결성 제어(주소 지정 가능). 전자적으로 전송된 전자적으로 보호되는 의료 정보가 폐기될 때까지 탐지 없이 부적절하게 수정되지 않도록 보안 조치를 취합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
164.312(e)(2)(i)	(i) 무결성 제어(주소 지정 가능). 전자적으로 전송된 전자적으로 보호되는 의료 정보가 폐기될 때까지 탐지 없이 부적절하게 수정되지 않도록 보안 조치를 취합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.312(e)(2)(ii)	(ii) 암호화(주소 지정 가능). 적절하다고 판단될 때마다 전자적으로 보호되는 의료 정보를 암호화하는 메커니즘을 구현합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(1)	(b)(1) 표준: 단체 건강보험 요건. 보험 후원자에게 공개된 유일한 전자적으로 보호된 의료 정보가 164.504(f)(1)(ii) 또는 (iii)에 따라 공개되거나 164.508에 따라 승인된 경우를 제외하고, 단체 건강보험의 보험 문서에는 다음 내용이 수록되어 있어야 합니다. 보험 후원자는 단체 건강보험을 대신하여 보험 후원자에게 또는 후원자에 의해 생성, 수신, 유지 또는 전송되는 전자적으로 보호되는 건강 정보를 합리적이고 적절하게 보호합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다. (ii) 164.504(f)(2)(iii)에서 요구하는 적절한 분리가 합리적이고 적절한 보안 조치로 뒷받침되는지 확인합니다.(iii) 이 정보를 제공하는 하청업체를 포함한 모든 대리인이 정보를 보호하기 위해 합리적이고 적절한 보안 조치를 구현하는 데 동의하는지 확인합니다.(iv) 보안 사고를 인지하게 되면 단체 건강보험에 보고합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	rds-cluster-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
164.314(b)(2)(i)	(2) 구현 사양(필수). 단체 건강보험의 보험 문서는 보험 후원자에게 다음을 요구하는 조항을 포함하도록 수정되어야 합니다. (i) 단체 건강보험을 대신하여 생성, 수신, 유지 또는 전송하는 전자적으로 보호되는 의료 정보의 기밀성, 무결성, 가용성을 합리적이고 적절하게 보호하는 관리적, 물리적, 기술적 보호 장치를 구현합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

템플릿

템플릿은 GitHub: HIPAA 보안 운영 모범 사례에서 확인할 수 있습니다.

IRS 1075 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 IRS 1075와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 IRS 1075 제어와 관련이 있습니다. 하나의 IRS 1075 제어가 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 d. 전송 중 데이터 암호화	FTI는 클라우드 환경 내에서 전송 중에 암호화되어야 합니다. FTI 암호화에 사용되는 모든 메커니즘은 FIPS 140 인증을 받아야 하며 최신 FIPS 140 준수 모듈을 사용하여 작동해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.3.1 클라우드 컴퓨팅 d. 전송 중 데이터 암호화	FTI는 클라우드 환경 내에서 전송 중에 암호화되어야 합니다. FTI 암호화에 사용되는 모든 메커니즘은 FIPS 140 인증을 받아야 하며 최신 FIPS 140 준	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC)

제어 ID	제어 설명	AWS 구성 규칙	지침
	수 모듈을 사용하여 작동해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.		내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.3.1 클라우드 컴퓨팅 d. 전송 중 데이터 암호화	FTI는 클라우드 환경 내에서 전송 중에 암호화되어야 합니다. FTI 암호화에 사용되는 모든 메커니즘은 FIPS 140 인증을 받아야 하며 최신 FIPS 140 준수 모듈을 사용하여 작동해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.3.1 클라우드 컴퓨팅 d. 전송 중 데이터 암호화	FTI는 클라우드 환경 내에서 전송 중에 암호화되어야 합니다. FTI 암호화에 사용되는 모든 메커니즘은 FIPS 140 인증을 받아야 하며 최신 FIPS 140 준수 모듈을 사용하여 작동해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 d. 전송 중 데이터 암호화	FTI는 클라우드 환경 내에서 전송 중에 암호화되어야 합니다. FTI 암호화에 사용되는 모든 메커니즘은 FIPS 140 인증을 받아야 하며 최신 FIPS 140 준수 모듈을 사용하여 작동해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.3.1 클라우드 컴퓨팅 d. 전송 중 데이터 암호화	FTI는 클라우드 환경 내에서 전송 중에 암호화되어야 합니다. FTI 암호화에 사용되는 모든 메커니즘은 FIPS 140 인증을 받아야 하며 최신 FIPS 140 준수 모듈을 사용하여 작동해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 d. 전송 중 데이터 암호화	FTI는 클라우드 환경 내에서 전송 중에 암호화되어야 합니다. FTI 암호화에 사용되는 모든 메커니즘은 FIPS 140 인증을 받아야 하며 최신 FIPS 140 준수 모듈을 사용하여 작동해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.3.1 클라우드 컴퓨팅 e. 저장 데이터 암호화	저장 데이터 암호화: 클라우드에 저장된 상태에서 최신 FIPS 140 인증 암호화 메커니즘을 사용하여 FTI를 암호화해야 합니다. 이 요구 사항은 SLA에 포함되어야 합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 k. 다중 인증	인터넷을 통해 클라우드 솔루션을 사용할 수 있는 경우(즉, 기관의 신뢰할 수 있는 네트워크 외부에서 클라우드 솔루션에 액세스할 수 있는 경우) 기관은 충분한 다중 인증을 구현해야 합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
3.3.1 클라우드 컴퓨팅 k. 다중 인증	인터넷을 통해 클라우드 솔루션을 사용할 수 있는 경우(즉, 기관의 신뢰할 수 있는 네트워크 외부에서 클라우드 솔루션에 액세스할 수 있는 경우) 기관은 충분한 다중 인증을 구현해야 합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 k. 다중 인증	인터넷을 통해 클라우드 솔루션을 사용할 수 있는 경우(즉, 기관의 신뢰할 수 있는 네트워크 외부에서 클라우드 솔루션에 액세스할 수 있는 경우) 기관은 충분한 다중 인증을 구현해야 합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
3.3.1 클라우드 컴퓨팅 k. 다중 인증	인터넷을 통해 클라우드 솔루션을 사용할 수 있는 경우(즉, 기관의 신뢰할 수 있는 네트워크 외부에서 클라우드 솔루션에 액세스할 수 있는 경우) 기관은 충분한 다중 인증을 구현해야 합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1 클라우드 컴퓨팅 i. 위험 평가	기관은 FTI 수신, 처리, 저장, 액세스, 보호 및/또는 전송에 사용되는 모든 정보 시스템에 적용되는 보안 및 개인정보보호 제어를 매년 평가해야 합니다.	annual-risk-assessment-performed(프로세스 확인)	조직에 대한 연간 위험 평가를 수행합니다. 위험 평가는 식별된 위험 및/또는 취약성이 조직에 영향을 미칠 가능성과 영향을 파악하는 데 도움이 될 수 있습니다.
3.6 네트워크 경계 및 인프라	기관은 FTI 및 FTI 시스템을 보호하기 위해 라우터, 방화벽, 스위치, 침입 탐지 시스템 등 시스템 아키텍처 전체에 경계 보호 디바이스를 구현해야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6 네트워크 경계 및 인프라	기관은 FTI 및 FTI 시스템을 보호하기 위해 라우터, 방화벽, 스위치, 침입 탐지 시스템 등 시스템 아키텍처 전체에 경계 보호 디바이스를 구현해야 합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
3.6 네트워크 경계 및 인프라	기관은 FTI 및 FTI 시스템을 보호하기 위해 라우터, 방화벽, 스위치, 침입 탐지 시스템 등 시스템 아키텍처 전체에 경계 보호 디바이스를 구현해야 합니다.	netfw-policy-rule-group-associated	AWS Network Firewall 정책은 방화벽이 Amazon VPC에서 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하여 패킷과 트래픽 흐름을 필터링하고 기본 트래픽 처리를 정의합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6 네트워크 경계 및 인프라	기관은 FTI 및 FTI 시스템을 보호하기 위해 라우터, 방화벽, 스위치, 침입 탐지 시스템 등 시스템 아키텍처 전체에 경계 보호 디바이스를 구현해야 합니다.	netfw-stateless-rule-group-not-empty	AWS Network Firewall 규칙 그룹에는 방화벽이 VPC에서 트래픽을 처리하는 방법을 정의하는 규칙이 포함되어 있습니다. 방화벽 정책에 있는 빈 상태 비저장 규칙 그룹은 트래픽을 처리하지 않습니다.
3.6 네트워크 경계 및 인프라	기관은 FTI 및 FTI 시스템을 보호하기 위해 라우터, 방화벽, 스위치, 침입 탐지 시스템 등 시스템 아키텍처 전체에 경계 보호 디바이스를 구현해야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6 네트워크 경계 및 인프라	기관은 FTI 및 FTI 시스템을 보호하기 위해 라우터, 방화벽, 스위치, 침입 탐지 시스템 등 시스템 아키텍처 전체에 경계 보호 디바이스를 구현해야 합니다.	waf-regional-rule-not-empty	AWS WAF에 비어 있지 않은 규칙이 있는지 확인합니다. 조건이 없는 규칙에는 의도하지 않은 동작이 발생할 수 있습니다.
3.6 네트워크 경계 및 인프라	기관은 FTI 및 FTI 시스템을 보호하기 위해 라우터, 방화벽, 스위치, 침입 탐지 시스템 등 시스템 아키텍처 전체에 경계 보호 디바이스를 구현해야 합니다.	waf-regional-rulegroup-not-empty	AWS WAF에 비어 있지 않은 규칙 그룹이 있는지 확인합니다. 규칙 그룹이 비어 있으면 의도하지 않은 동작이 발생할 수 있습니다.
3.6 네트워크 경계 및 인프라	기관은 FTI 및 FTI 시스템을 보호하기 위해 라우터, 방화벽, 스위치, 침입 탐지 시스템 등 시스템 아키텍처 전체에 경계 보호 디바이스를 구현해야 합니다.	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6 네트워크 경계 및 인프라	기관은 FTI 및 FTI 시스템을 보호하기 위해 라우터, 방화벽, 스위치, 침입 탐지 시스템 등 시스템 아키텍처 전체에 경계 보호 디바이스를 구현해야 합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
3.6 네트워크 경계 및 인프라	기관은 FTI 및 FTI 시스템을 보호하기 위해 라우터, 방화벽, 스위치, 침입 탐지 시스템 등 시스템 아키텍처 전체에 경계 보호 디바이스를 구현해야 합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (f)	기관 계정 관리 절차 사전 요구 사항에 따라 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AC-2 계정 관리 (f)	기관 계정 관리 절차 사전 요구 사항에 따라 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (f)	기관 계정 관리 절차 사전 요구 사항에 따라 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
AC-2 계정 관리 (f)	기관 계정 관리 절차 사전 요구 사항에 따라 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (f)	기관 계정 관리 절차 사전 요구 사항에 따라 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-2 계정 관리 (g)	계정 사용 모니터링	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (g)	계정 사용 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AC-2 계정 관리 (g)	계정 사용 모니터링	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (g)	계정 사용 모니터링	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AC-2 계정 관리 (g)	계정 사용 모니터링	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (g)	계정 사용 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (g)	계정 사용 모니터링	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (g)	계정 사용 모니터링	securityhub-enabled	AWS Security Hub 는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (j)	계정이 계정 관리 요구 사항을 준수하는지 검토합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AC-2 계정 관리 (j)	계정이 계정 관리 요구 사항을 준수하는지 검토합니다.	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (j)	계정이 계정 관리 요구 사항을 준수하는지 검토합니다.	secretsmanager-secret-periodic-rotation	이 규칙은 AWS Secrets Manager 보안 암호에 주기적 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다. 기본값은 90일입니다.
AC-2 계정 관리 (j)	계정이 계정 관리 요구 사항을 준수하는지 검토합니다.	secretsmanager-secret-unused	AWS Secrets Manager에 미사용 자격 증명이 있는 경우 자격 증명을 비활성화 및/또는 제거해야 합니다. 최소 권한 원칙을 위반할 수 있습니다. 이 규칙을 사용하면 값을 unusedForDays(Config 기본값: 90)로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (j)	계정이 계정 관리 요구 사항을 준수하는지 검토합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2 계정 관리 (j)	계정이 계정 관리 요구 사항을 준수하는지 검토합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AC-2 계정 관리 (j)	계정이 계정 관리 요구 사항을 준수하는지 검토합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (j)	계정이 계정 관리 요구 사항을 준수하는지 검토합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2 계정 관리 (j)	계정이 계정 관리 요구 사항을 준수하는지 검토합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2 계정 관리 (j)	계정이 계정 관리 요구 사항을 준수하는지 검토합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-2 계정 관리 (j)	계정이 계정 관리 요구 사항을 준수하는지 검토합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
(CE-1) 자동화된 시스템 계정 관리	자동화된 메커니즘을 사용하여 시스템 계정 관리를 지원합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
(CE-1) 자동화된 시스템 계정 관리	자동화된 메커니즘을 사용하여 시스템 계정 관리를 지원합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
(CE-1) 자동화된 시스템 계정 관리	자동화된 메커니즘을 사용하여 시스템 계정 관리를 지원합니다.	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
(CE-3): 계정 비활성화	계정이 다음과 같은 경우 120일 이내에 계정을 비활성화합니다. a. 만료되었습니다. b. 더 이상 사용자 또는 개인과 관련이 없습니다. c. 조직 정책을 위반합니다. d. 비권한 계정의 경우 120일, 권한 있는 계정의 경우 60일 동안 비활성 상태였습니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
(CE-12) 이례적 사용에 대한 계정 모니터링	기관에서 정의한 이례적 사용이 있는지 시스템 계정을 모니터링하고, 기관에서 정의한 직원 또는 역할에 시스템 계정의 이례적 사용을 보고합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	secretsmanager-secret-unused	AWS Secrets Manager에 미사용 자격 증명이 있는 경우 자격 증명을 비활성화 및/또는 제거해야 합니다. 최소 권한 원칙을 위반할 수 있습니다. 이 규칙을 사용하면 값을 unusedForDays(Config 기본값: 90)로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	codebuild-project-environment-privileged-check	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있지 않은지 확인합니다. Docker API와 컨테이너의 기본 하드웨어에 대해 의도하지 않은 액세스를 방지하려면 이 설정을 비활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ecs-containers-non privileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6 최소 권한	최소 권한 원칙을 이용하여 조직에서 할당한 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17: 원격 액세스	허용되는 각 원격 액세스 유형에 대한 사용 제한, 구성/연결 요구 사항 및 구현 지침을 설정하고 문서화하고, 이러한 연결을 허용하기 전에 시스템에 대한 각 유형의 원격 액세스를 승인합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.
AT-1: 인식 및 교육	시스템 사용자(관리자, 고위 경영진 및 계약업체 포함)에게 보안 및 개인정보보호 능력 교육 제공	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지하세요. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.
AU-2: 이벤트 감사	시스템에서 감사 기능이 지원되며 로깅할 수 있는 이벤트 유형을 확인합니다.	audit-log-policy-exists(프로세스 확인)	조직의 로깅 요구 사항을 정의하는 감사 로그 관리 정책을 수립하고 유지 관리합니다. 여기에는 감사 로그의 검토 및 보존이 포함되며 이에 국한되지는 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-16: 조직 간 감사 로깅	감사 정보가 조직 경계를 넘어 전송되는 경우 기관이 정의한 감사 정보를 외부 조직들 간에 조정하기 위해 기관에서 정의한 방법을 사용합니다.	audit-log-policy-exists(프로세스 확인)	조직의 로깅 요구 사항을 정의하는 감사 로그 관리 정책을 수립하고 유지 관리합니다. 여기에는 감사 로그의 검토 및 보존이 포함되며 이에 국한되지는 않습니다.
CA-7: 지속적 모니터링	시스템 수준의 지속적인 모니터링 전략을 개발하고 조직 수준의 지속적인 모니터링 전략에 따라 지속적인 모니터링을 구현합니다. 다음과 같이 모니터링할 기관 정의 지표를 설정합니다. 지속적인 모니터링 전략에 따라 지속적인 제어 평가. 지속적인 모니터링 전략에 따라 시스템 및 조직이 정의한 지표를 지속적으로 모니터링. 제어 평가 및 모니터링을 통해 생성된 정보의 상관관계 분석. 제어 평가 및 모니터링 정보 분석 결과를 다루기 위한 대응 조치. 최소한 매년 기관에서 정의한 담당자에게 시스템의 보안 및 개인정보보호 상태를 보고.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
CP-9: 시스템 백업	a. 보안 관련 문서를 포함하여 시스템 문서에 포함된 사용자 수준 정보를 매주 백업합니다. b. 시스템에 포함된 시스템 수준 정보를 매주 백업합니다. c. 보안 및 개인정보보호 관련 문서를 포함한 시스템 설명서를 매주 백업합니다. d. 백업 정보의 기밀성, 무결성 및 가용성을 보호합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2: 식별 및 인증(기관 사용자) (CE-1) 권한 있는 계정에 대한 다중 인증	권한 있는 계정에 대한 액세스를 위한 다중 인증 구현	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA-2: 식별 및 인증(기관 사용자) (CE-1) 권한 있는 계정에 대한 다중 인증	권한 있는 계정에 대한 액세스를 위한 다중 인증 구현	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2: 식별 및 인증(기관 사용자) (CE-2) 권한 없는 계정에 대한 다중 인증	권한 없는 계정에 대한 액세스를 위한 다중 인증을 구현합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-5: 인증자 관리: (CE-1) 암호 기반 인증: 암호 기반 인증용	다음과 같은 구성 및 복잡성 규칙을 적용합니다. 1. 최소 암호 길이를 14자로 설정합니다. 2. 숫자, 대문자, 소문자 및 특수 문자의 조합을 포함하도록 암호 복잡성을 최소화하세요. 3. 사용할 새 암호를 선택할 때는 최소 1글자 변경을 적용합니다. 4. 암호로 보호된 암호만 저장하고 전송합니다. 5. 암호 수명 제한을 적용합니다. i. 최소 1일, 최대 90일. ii. 서비스 계정 암호는 366일(포함) 이내에 만료됩니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
PM-5: 시스템 인벤토리	조직 시스템 인벤토리를 지속적으로 개발하고 업데이트합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PM-5: 시스템 인벤토리	조직 시스템 인벤토리를 지속적으로 개발하고 업데이트합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
PM-5: 시스템 인벤토리	조직 시스템 인벤토리를 지속적으로 개발하고 업데이트합니다.	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PM-5: 시스템 인벤토리	조직 시스템 인벤토리를 지속적으로 개발하고 업데이트합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
RA-5: 취약성 모니터링 및 스캔	기관 네트워크에 새 정보 시스템을 배치하기 전에 30일마다 시스템 및 호스팅된 애플리케이션의 취약성을 모니터링하고 스캔하여 수정 조치 및 시스템에 잠재적으로 영향을 미칠 수 있는 새로운 취약성이 식별되고 보고되는 시기를 확인합니다.	vuln-scans-performed(프로세스 확인)	규정 준수 요구 사항에 따라 취약성 스캔이 수행되는지 확인합니다. 검사 주기, 사용하는 도구, 결과 사용은 조직에서 정의해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10: 개발자 구성 관리 (e.)	시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SA-10: 개발자 구성 관리 (e.)	시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10: 개발자 구성 관리 (e.)	시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-10: 개발자 구성 관리 (a) (c.)	시스템, 구성 요소 또는 서비스 설계, 개발, 구현, 운영 중에 구성 관리를 수행합니다. 시스템, 구성 요소 또는 서비스에 대해 조직이 승인한 변경 사항만 구현합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
SC-4: 공유 시스템 리소스의 정보	공유 시스템 리소스의 무단 및 의도하지 않은 정보 전송을 방지합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7: 경계 보호	시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링 및 제어합니다. 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 하위 네트워크를 내부 조직 네트워크와 분리합니다. 조직 보안 아키텍처에 따라 배치된 경계 보호 디바이스로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7: 경계 보호 (CE-9) 위협적인 발신 통신 트래픽 제한	외부 시스템에 위협이 되는 발신 통신 트래픽을 탐지 및 거부하고, 거부된 통신과 관련된 내부 사용자의 신원을 감사합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
SC-7: 경계 보호 (CE-9) 위협적인 발신 통신 트래픽 제한	외부 시스템에 위협이 되는 발신 통신 트래픽을 탐지 및 거부하고, 거부된 통신과 관련된 내부 사용자의 신원을 감사합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7: 경계 보호 (CE-9) 위협적인 발신 통신 트래픽 제한	외부 시스템에 위협이 되는 발신 통신 트래픽을 탐지 및 거부하고, 거부된 통신과 관련된 내부 사용자의 신원을 감사합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
SC-7: 경계 보호 (IRS에서 정의)	기관은 신뢰 경계에서 경계 보호(일반적으로 방화벽 사용)를 구현하고 관리해야 합니다. 각 신뢰 경계를 모니터링하고 각 경계에 걸친 통신을 통제해야 합니다.	netfw-policy-rule-group-associated	AWS Network Firewall 정책은 방화벽이 Amazon VPC에서 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하여 패킷과 트래픽 흐름을 필터링하고 기본 트래픽 처리를 정의합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7: 경계 보호 (IRS에서 정의)	기관은 신뢰 경계에서 경계 보호(일반적으로 방화벽 사용)를 구현하고 관리해야 합니다. 각 신뢰 경계를 모니터링하고 각 경계에 걸친 통신을 통제해야 합니다.	netfw-stateless-rule-group-not-empty	AWS Network Firewall 규칙 그룹에는 방화벽이 VPC에서 트래픽을 처리하는 방법을 정의하는 규칙이 포함되어 있습니다. 방화벽 정책에 있는 빈 상태 비저장 규칙 그룹은 트래픽을 처리하지 않습니다.
SC-8: 전송 기밀성 및 무결성 (CE-1) 암호화 보호	정보의 무단 공개를 방지하고 전송 중 정보 변경을 감지하는 암호화 메커니즘을 구현합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8: 전송 기밀성 및 무결성 (CE-1) 암호화 보호	정보의 무단 공개를 방지하고 전송 중 정보 변경을 감지하는 암호화 메커니즘을 구현합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8: 전송 기밀성 및 무결성 (CE-1) 암호화 보호	정보의 무단 공개를 방지하고 전송 중 정보 변경을 감지하는 암호화 메커니즘을 구현합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8: 전송 기밀성 및 무결성 (CE-1) 암호화 보호	정보의 무단 공개를 방지하고 전송 중 정보 변경을 감지하는 암호화 메커니즘을 구현합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8: 전송 기밀성 및 무결성 (CE-1) 암호화 보호	정보의 무단 공개를 방지하고 전송 중 정보 변경을 감지하는 암호화 메커니즘을 구현합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8: 전송 기밀성 및 무결성 (CE-1) 암호화 보호	정보의 무단 공개를 방지하고 전송 중 정보 변경을 감지하는 암호화 메커니즘을 구현합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8: 전송 기밀성 및 무결성 (CE-1) 암호화 보호	정보의 무단 공개를 방지하고 전송 중 정보 변경을 감지하는 암호화 메커니즘을 구현합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-12: 암호화 키 설정 및 관리	기관은 시스템 내에서 암호화를 사용할 때 NIST SP 800-57, 키 생성, 배포, 저장, 액세스 및 폐기를 위한 키 관리 권장 사항 등의 키 관리 요구 사항에 따라 암호화 키를 설정하고 관리해야 합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-12: 암호화 키 설정 및 관리	기관은 시스템 내에서 암호화를 사용할 때 NIST SP 800-57, 키 생성, 배포, 저장, 액세스 및 폐기를 위한 키 관리 권장 사항 등의 키 관리 요구 사항에 따라 암호화 키를 설정하고 관리해야 합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13: 암호화 보호	지정된 각 암호화 사용에 필요한 다음 유형의 암호화를 구현합니다. 최신 FIPS-140 검증 암호화 메커니즘, NIST 800-52, 전송 계층 보안(TLS) 구현, 전송 중 암호화(페이로드 암호화)의 선택, 구성 및 사용에 대한 지침. 디지털 서명에 SHA-1 사용을 금지합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23: 세션 인증	통신 세션의 신뢰성을 보호합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28: 저장된 정보 보호 (CE-1) 암호화 보호	비휘발성 스토리지의 최종 사용자 컴퓨팅 시스템(예: 데스크톱 컴퓨터, 랩톱 컴퓨터, 모바일 디바이스, 휴대용 및 이동식 저장 장치)에 저장된 FTI의 무단 공개 및 수정을 방지하는 암호화 메커니즘을 구현합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2: 결함 수정 (IRS 정의)	기관은 매일 전원을 켜고 기관 네트워크에 연결할 때 워크스테이션(정책에 정의되어 있고 GFE 워크스테이션을 사용한 원격 연결 포함)을 점검하여 기관에서 승인한 최신 패치가 적용되었는지, 없는 패치나 새 패치가 필요에 따라 적용되었는지 또는 적어도 매 24시간에 한 번 점검이 완료되었는지 확인해야 합니다(주말, 공휴일 등 제외).	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2: 결함 수정 (IRS 정의)	기관은 매일 전원을 켜고 기관 네트워크에 연결할 때 워크스테이션(정책에 정의되어 있고 GFE 워크스테이션을 사용한 원격 연결 포함)을 점검하여 기관에서 승인한 최신 패치가 적용되었는지, 없는 패치나 새 패치가 필요에 따라 적용되었는지 또는 적어도 매 24시간에 한 번 점검이 완료되었는지 확인해야 합니다(주말, 공휴일 등 제외).	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
SI-2: 결함 수정 (IRS 정의)	기관은 매일 전원을 켜고 기관 네트워크에 연결할 때 워크스테이션(정책에 정의되어 있고 GFE 워크스테이션을 사용한 원격 연결 포함)을 점검하여 기관에서 승인한 최신 패치가 적용되었는지, 없는 패치나 새 패치가 필요에 따라 적용되었는지 또는 적어도 매 24시간에 한 번 점검이 완료되었는지 확인해야 합니다(주말, 공휴일 등 제외).	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2: 결함 수정 (IRS 정의)	기관은 매일 전원을 켜고 기관 네트워크에 연결할 때 워크스테이션(정책에 정의되어 있고 GFE 워크스테이션을 사용한 원격 연결 포함)을 점검하여 기관에서 승인한 최신 패치가 적용되었는지, 없는 패치나 새 패치가 필요에 따라 적용되었는지 또는 적어도 매 24시간에 한 번 점검이 완료되었는지 확인해야 합니다(주말, 공휴일 등 제외).	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. AWS Fargate 플랫폼 버전에 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.
SI-2: 결함 수정 (IRS 정의)	기관은 매일 전원을 켜고 기관 네트워크에 연결할 때 워크스테이션(정책에 정의되어 있고 GFE 워크스테이션을 사용한 원격 연결 포함)을 점검하여 기관에서 승인한 최신 패치가 적용되었는지, 없는 패치나 새 패치가 필요에 따라 적용되었는지 또는 적어도 매 24시간에 한 번 점검이 완료되었는지 확인해야 합니다(주말, 공휴일 등 제외).	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2: 결함 수정 (IRS 정의)	기관은 매일 전원을 켜고 기관 네트워크에 연결할 때 워크스테이션(정책에 정의되어 있고 GFE 워크스테이션을 사용한 원격 연결 포함)을 점검하여 기관에서 승인한 최신 패치가 적용되었는지, 없는 패치나 새 패치가 필요에 따라 적용되었는지 또는 적어도 매 24시간에 한 번 점검이 완료되었는지 확인해야 합니다(주말, 공휴일 등 제외).	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4: 시스템 모니터링	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1.[과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2.승인되지 않은 로컬, 네트워크 및 원격 연결. b. [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 모니터링 디바이스 배포: 1. 정보 시스템 내에서 조직이 결정한 필수 정보를 전략적으로 수집합니다. 2. 시스템 내의 임시 위치에서 조직이 관심을 갖는 특정 유형의 트랜잭션을 추적합니다. d. 침입 모니터링 도구를 통해 획득한 정보를 무단 액세스, 수정 및 삭제로부터 보호합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4: 시스템 모니터링	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1.[과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2.승인되지 않은 로컬, 네트워크 및 원격 연결. b. [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 모니터링 디바이스 배포: 1. 정보 시스템 내에서 조직이 결정한 필수 정보를 전략적으로 수집합니다. 2. 시스템 내의 임시 위치에서 조직이 관심을 갖는 특정 유형의 트랜잭션을 추적합니다. d. 침입 모니터링 도구를 통해 획득한 정보를 무단 액세스, 수정 및 삭제로부터 보호합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4: 시스템 모니터링	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1.[과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2.승인되지 않은 로컬, 네트워크 및 원격 연결. b. [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 모니터링 디바이스 배포: 1. 정보 시스템 내에서 조직이 결정한 필수 정보를 전략적으로 수집합니다. 2. 시스템 내의 임시 위치에서 조직이 관심을 갖는 특정 유형의 트랜잭션을 추적합니다. d. 침입 모니터링 도구를 통해 획득한 정보를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4: 시스템 모니터링	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1.[과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2.승인되지 않은 로컬, 네트워크 및 원격 연결. b. [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 모니터링 디바이스 배포: 1. 정보 시스템 내에서 조직이 결정한 필수 정보를 전략적으로 수집합니다. 2. 시스템 내의 임시 위치에서 조직이 관심을 갖는 특정 유형의 트랜잭션을 추적합니다. d. 침입 모니터링 도구를 통해 획득한 정보를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4: 시스템 모니터링	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1.[과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2.승인되지 않은 로컬, 네트워크 및 원격 연결. b. [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 모니터링 디바이스 배포: 1. 정보 시스템 내에서 조직이 결정한 필수 정보를 전략적으로 수집합니다. 2. 시스템 내의 임시 위치에서 조직이 관심을 갖는 특정 유형의 트랜잭션을 추적합니다. d. 침입 모니터링 도구를 통해 획득한 정보를 무단 액세스, 수정 및 삭제로부터 보호합니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4: 시스템 모니터링 (IRS에서 정의)	모든 인터넷 액세스 포인트/포털은 기관 CISO의 승인에 따라 승인된 인터넷 “익명” 연결을 제외하고 인바운드 및 아웃바운드 트래픽 헤더 정보를 캡처하고 최소 1년 동안 보관해야 합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
SI-4: 시스템 모니터링 (IRS에서 정의)	모든 인터넷 액세스 포인트/포털은 기관 CISO의 승인에 따라 승인된 인터넷 “익명” 연결을 제외하고 인바운드 및 아웃바운드 트래픽 헤더 정보를 캡처하고 최소 1년 동안 보관해야 합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4: 시스템 모니터링 (IRS에서 정의)	모든 인터넷 액세스 포인트/포털은 기관 CISO의 승인에 따라 승인된 인터넷 “익명” 연결을 제외하고 인바운드 및 아웃바운드 트래픽 헤더 정보를 캡처하고 최소 1년 동안 보관해야 합니다.	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.
SI-4: 시스템 모니터링 (IRS에서 정의)	모든 인터넷 액세스 포인트/포털은 기관 CISO의 승인에 따라 승인된 인터넷 “익명” 연결을 제외하고 인바운드 및 아웃바운드 트래픽 헤더 정보를 캡처하고 최소 1년 동안 보관해야 합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4: 시스템 모니터링 (IRS에서 정의)	모든 인터넷 액세스 포인트/포털은 기관 CISO의 승인에 따라 승인된 인터넷 “익명” 연결을 제외하고 인바운드 및 아웃바운드 트래픽 헤더 정보를 캡처하고 최소 1년 동안 보관해야 합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
SI-4: 시스템 모니터링 (IRS에서 정의)	모든 인터넷 액세스 포인트/포털은 기관 CISO의 승인에 따라 승인된 인터넷 “익명” 연결을 제외하고 인바운드 및 아웃바운드 트래픽 헤더 정보를 캡처하고 최소 1년 동안 보관해야 합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4: 시스템 모니터링 (IRS에서 정의)	모든 인터넷 액세스 포인트/포털은 기관 CISO의 승인에 따라 승인된 인터넷 “익명” 연결을 제외하고 인바운드 및 아웃바운드 트래픽 헤더 정보를 캡처하고 최소 1년 동안 보관해야 합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
SI-4: 시스템 모니터링 (IRS에서 정의)	모든 인터넷 액세스 포인트/포털은 기관 CISO의 승인에 따라 승인된 인터넷 “익명” 연결을 제외하고 인바운드 및 아웃바운드 트래픽 헤더 정보를 캡처하고 최소 1년 동안 보관해야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
SI-4: 시스템 모니터링 (IRS에서 정의)	모든 인터넷 액세스 포인트/포털은 기관 CISO의 승인에 따라 승인된 인터넷 “익명” 연결을 제외하고 인바운드 및 아웃바운드 트래픽 헤더 정보를 캡처하고 최소 1년 동안 보관해야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4: 시스템 모니터링 (IRS에서 정의)	모든 인터넷 액세스 포인트/포털은 기관 CISO의 승인에 따라 승인된 인터넷 “익명” 연결을 제외하고 인바운드 및 아웃바운드 트래픽 헤더 정보를 캡처하고 최소 1년 동안 보관해야 합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
SI-4: 시스템 모니터링 (IRS에서 정의)	모든 인터넷 액세스 포인트/포털은 기관 CISO의 승인에 따라 승인된 인터넷 “익명” 연결을 제외하고 인바운드 및 아웃바운드 트래픽 헤더 정보를 캡처하고 최소 1년 동안 보관해야 합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7: 소프트웨어, 펌웨어 및 정보 무결성	무결성 검증 도구를 사용하여 시스템 커널, 드라이버, 펌웨어(예: BIOS, UEFI), 소프트웨어(예: OS, 애플리케이션, 미들웨어), 보안 속성 등의 소프트웨어, 펌웨어 및 정보에 대한 무단 변경을 탐지합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
SI-7: 소프트웨어, 펌웨어 및 정보 무결성	무결성 검증 도구를 사용하여 시스템 커널, 드라이버, 펌웨어(예: BIOS, UEFI), 소프트웨어(예: OS, 애플리케이션, 미들웨어), 보안 속성 등의 소프트웨어, 펌웨어 및 정보에 대한 무단 변경을 탐지합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7: 소프트웨어, 펌웨어 및 정보 무결성	무결성 검증 도구를 사용하여 시스템 커널, 드라이버, 펌웨어(예: BIOS, UEFI), 소프트웨어(예: OS, 애플리케이션, 미들웨어), 보안 속성 등의 소프트웨어, 펌웨어 및 정보에 대한 무단 변경을 탐지합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	dynamodb-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	ebs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	efs-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	rds-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	s3-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
SI-12: 정보 관리 및 보존	해당 법률, 행정 명령, 지침, 규정, 정책, 표준, 가이드라인 및 운영 요구 사항에 따라 시스템 내의 정보와 시스템에서 출력되는 정보를 관리하고 유지합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.

템플릿

템플릿은 GitHub: IRS 1075 운영 모범 사례에서 확인할 수 있습니다.

K-ISMS 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 한국 - 정보 보안 관리 시스템(ISMS)과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 한국 - ISMS 제어와 관련이 있습니다. 하나의 한국 - ISMS 제어가 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	AWS 구성 규칙	지침
1.2.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
1.2.1	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.1.3	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
2.1.3	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
2.3.3	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
2.3.3	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
2.5.1	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
2.5.1	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
2.5.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
2.5.1	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	AWS 구성 규칙	지침
2.5.1	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
2.5.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.5.1	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
2.5.1	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
2.5.1	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	AWS 구성 규칙	지침
2.5.1	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
2.5.1	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
2.5.1	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
2.5.1	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
2.5.1	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.5.3	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	AWS 구성 규칙	지침
2.5.3	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
2.5.3	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
2.5.4	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.
2.5.5	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.5.5	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
2.5.5	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
2.6	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
2.6	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	AWS 구성 규칙	지침
2.6	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
2.6	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
2.6	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	AWS 구성 규칙	지침
2.6	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
2.6	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.6	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
2.6	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.6	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
2.6	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
2.6	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
2.6	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
2.6	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
2.6	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
2.6	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
2.6	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
2.6	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
2.6	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
2.6	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
2.6.6	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
2.6.6	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
2.6.6	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
2.6.6	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
2.6.6	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
2.6.6	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
2.6.6	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
2.6.6	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
2.6.6	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
2.6.6	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
2.6.6	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
2.6.6	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
2.6.7	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
2.7	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
2.7	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.7	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.7	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
2.7	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
2.7	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
2.7	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
2.7	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.7	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
2.7	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
2.7	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.7	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
2.7	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
2.7	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
2.7	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.7	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
2.7	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
2.7	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.7	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
2.7	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.7	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.7	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
2.7	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.7	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
2.7	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
2.7.1	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
2.7.1	elb-predefined-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic Elastic Load Balancing SSL 리스너가 사전 정의된 보안 정책을 사용하고 있는지 확인합니다. Elastic Load Balancing은 클라이언트와 로드 밸런서 간에 연결을 설정할 때 SSL 협상에 사용되는 사전 정의된 SSL 협상 구성을 제공합니다. SSL 협상 구성은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 이 규칙을 사용하려면 SSL 리스너에 대해 사전 정의된 보안 정책을 설정해야 합니다. 기본 보안 정책은 ELBSecurityPolicy-TLS-1-2-2017-0입니다. 실제 값은 조직의 정책을 반영해야 합니다.
2.7.2	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	AWS 구성 규칙	지침
2.7.2	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
2.8.5	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
2.8.5	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	AWS 구성 규칙	지침
2.8.6	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
2.8.6	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
2.9.1	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.9.1	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail의 사용이 포함됩니다.
2.9.1	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	AWS 구성 규칙	지침
2.9.1	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
2.9.2	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	AWS 구성 규칙	지침
2.9.2	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
2.9.2	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
2.9.2	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
2.9.2	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.9.2	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.
2.9.3	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.9.3	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
2.9.3	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.
2.9.3	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.9.3	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
2.9.3	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
2.9.3	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.9.3	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
2.9.3	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
2.9.3	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.9.3	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
2.9.3	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.

제어 ID	AWS 구성 규칙	지침
2.9.3	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
2.9.3	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
2.9.3	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
2.9.3	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.9.3	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.
2.9.4	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
2.9.4	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
2.9.4	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
2.9.4	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
2.9.4	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
2.9.4	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
2.9.4	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
2.9.4	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.9.4	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
2.9.4	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
2.9.4	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
2.10.3	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
2.10.3	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
2.10.3	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
2.10.3	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
2.10.3	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.10.5	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.10.5	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.10.5	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
2.10.5	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
2.10.5	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.10.5	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
2.10.5	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.10.5	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.10.8	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.10.8	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
2.11.2	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.11.3	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
2.11.3	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
2.11.3	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
2.11.3	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.
2.11.3	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	AWS 구성 규칙	지침
2.11.3	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
2.12	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.12	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
2.12	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.
2.12	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.12	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
2.12	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
2.12	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.12	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
2.12	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
2.12	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.12	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
2.12	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	AWS 구성 규칙	지침
2.12	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.
2.12	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
2.12	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
2.12	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
2.12	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.12	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

템플릿

템플릿은 GitHub: K-ISMS 운영 모범 사례에서 확인할 수 있습니다.

로드 밸런싱 운영 모범 사례

이 적합성 팩에는 내부의 로드 밸런싱을 기반으로 하는 AWS Config 규칙이 포함되어 있습니다 AWS. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 로드 밸런싱 운영 모범 사례에서 확인할 수 있습니다.

로깅 운영 모범 사례

이 적합성 팩에는 로깅 기반 AWS Config 규칙이 포함되어 있습니다 AWS. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 로깅을 위한 운영 모범 사례에서 사용할 수 있습니다.

관리 및 거버넌스 서비스 운영 모범 사례

이 적합성 팩에는 관리 및 거버넌스 서비스에 기반한 AWS Config 규칙이 포함되어 있습니다. 자세한 내용은 의 관리 및 거버넌스 AWS를 참조하세요. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 관리 및 거버넌스 서비스의 운영 모범 사례에서 확인할 수 있습니다.

MAS Notice 655 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 싱가포르 통화청(MAS) 공지 655 - 사이버 위생 및 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 MAS 공지 655 - 사이버 위생 제어와 관련이 있습니다. MAS Notice 655 — 사이버 위생 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	AWS 구성 규칙	지침
4.1	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과

제어 ID	AWS 구성 규칙	지침
		도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
4.1	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
4.1	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
4.1	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
4.1	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
4.1	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
4.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
4.1	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
4.1	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	AWS 구성 규칙	지침
4.1	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
4.1	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
4.1	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
4.1	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
4.1	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
4.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
4.1	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
4.1	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
4.1	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
4.1	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
4.1	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
4.2	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
4.2	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	AWS 구성 규칙	지침
4.2	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
4.2	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
4.2	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
4.2	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
4.2	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
4.2	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository(ECR) 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.
4.3	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	AWS 구성 규칙	지침
4.3	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
4.3	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
4.3	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
4.4	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
4.4	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
4.4	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
4.4	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
4.4	ec2-security-group-attached-to-eni-periodic	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
4.4	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
4.4	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
4.4	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
4.4	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
4.4	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
4.4	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
4.4	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
4.4	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	AWS 구성 규칙	지침
4.4	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
4.4	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
4.4	waf-regional-rule-not-empty	AWS WAF에 비어 있지 않은 규칙이 있는지 확인합니다. 조건이 없는 규칙에는 의도하지 않은 동작이 발생할 수 있습니다.
4.4	waf-regional-rulegroup-not-empty	AWS WAF에 비어 있지 않은 규칙 그룹이 있는지 확인합니다. 규칙 그룹이 비어 있으면 의도하지 않은 동작이 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
4.4	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.
4.4	netfw-policy-default-action-fragment-packets	AWS Network Firewall 정책은 방화벽이 Amazon VPC에서 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 패킷과 트래픽 흐름을 필터링하도록 상태 비저장 및 상태 저장 규칙 그룹을 구성합니다. Pass 작업을 기본값으로 설정하면 의도하지 않은 트래픽이 허용될 수 있습니다.
4.4	netfw-policy-default-action-full-packets	AWS Network Firewall 정책은 방화벽이 Amazon VPC에서 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 패킷과 트래픽 흐름을 필터링하도록 상태 비저장 및 상태 저장 규칙 그룹을 구성합니다. Pass 작업을 기본값으로 설정하면 의도하지 않은 트래픽이 허용될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
4.4	netfw-policy-rule-group-associated	AWS Network Firewall 정책은 방화벽이 Amazon VPC에서 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하여 패킷과 트래픽 흐름을 필터링하고 기본 트래픽 처리를 정의합니다.
4.4	netfw-stateless-rule-group-not-empty	AWS Network Firewall 규칙 그룹에는 방화벽이 VPC에서 트래픽을 처리하는 방법을 정의하는 규칙이 포함되어 있습니다. 방화벽 정책에 있는 빈 상태 비저장 규칙 그룹은 트래픽을 처리하지 않습니다.
4.4	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
4.4	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
4.4	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
4.4	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
4.4	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
4.4	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
4.4	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
4.4	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
4.4	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
4.4	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
4.4	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
4.4	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
4.4	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	AWS 구성 규칙	지침
4.4	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
4.4	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
4.4	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
4.5	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	AWS 구성 규칙	지침
4.5	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
4.5	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
4.5	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
4.6	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
4.6	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
4.6	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
4.6	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
4.6	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
4.6	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

템플릿

템플릿은 GitHub: MAS Notice 655 운영 모범 사례에서 확인할 수 있습니다.

MAS TRMG 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계

되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 2021년 1월 싱가포르 통화청(MAS) 기술 위험 관리 지침(TRMG)과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 AWS Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 MAS TRMG 제어와 관련이 있습니다. MAS TRMG 2021년 1월 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	AWS 구성 규칙	지침
3.3.1	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
5.4.3	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
5.4.3	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대

제어 ID	AWS 구성 규칙	지침
		신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
6.1.1	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
6.1.2	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
6.1.4	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
6.1.4	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
6.1.4	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager 에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
6.2.1	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
6.3.1	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	AWS 구성 규칙	지침
6.4.5	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
6.4.5	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
6.4.5	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
6.4.5	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	AWS 구성 규칙	지침
6.4.5	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
6.4.5	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
6.4.5	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
6.4.5	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
6.4.5	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
6.4.5	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	AWS 구성 규칙	지침
6.4.5	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
6.4.5	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
6.4.6	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
6.4.6	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
6.4.6	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
6.4.6	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	AWS 구성 규칙	지침
6.4.6	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
6.4.6	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	AWS 구성 규칙	지침
6.4.6	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
6.4.6	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
6.4.6	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
6.4.6	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
6.4.7	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
6.4.7	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
6.4.7	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
6.4.7	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	AWS 구성 규칙	지침
6.4.7	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
6.4.7	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail의 사용이 포함됩니다.
6.4.7	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	AWS 구성 규칙	지침
6.4.7	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
6.4.7	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
6.4.7	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
6.4.7	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
6.4.7	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
6.4.7	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
6.4.7	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
6.4.7	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	AWS 구성 규칙	지침
6.4.8	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
6.4.8	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
6.4.8	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
6.4.8	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
6.4.8	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
6.4.8	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
6.4.8	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
6.4.8	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
7.2.1	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	AWS 구성 규칙	지침
7.2.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
7.4.1	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	AWS 구성 규칙	지침
7.4.1	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
7.4.1	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
7.4.1	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	AWS 구성 규칙	지침
7.4.1	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
7.4.1	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
7.5.5	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
7.5.5	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
7.5.5	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	AWS 구성 규칙	지침
7.5.5	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
7.5.5	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
7.5.5	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
7.5.5	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
7.5.5	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
7.5.5	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
7.5.5	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
7.5.7	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
7.5.7	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
7.5.7	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
7.5.7	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
7.5.7	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
7.5.7	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
7.5.7	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
7.5.7	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
7.5.7	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
7.5.7	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
7.5.7	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
7.5.7	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
8.1.1	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
8.1.1	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
8.1.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
8.1.1	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
8.1.1	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
8.1.1	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
8.1.1	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
8.1.1	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
8.1.2	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
8.1.2	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.
8.1.2	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
8.1.2	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service(OpenSearch Service)의 고가용성과 내결함성을 위해서는 최소한 3개 이상의 데이터 노드가 필요합니다. 3개 이상의 데이터 노드가 포함된 OpenSearch Service 도메인을 배포하면 노드에 장애가 발생하더라도 클러스터 운영이 보장됩니다.
8.1.2	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
8.1.3	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
8.1.3	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 강화된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
8.1.3	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
8.1.3	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
8.4.1	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
8.4.1	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
8.4.1	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
8.4.1	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.
8.4.1	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	AWS 구성 규칙	지침
8.4.1	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
8.4.1	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
8.4.1	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
8.4.1	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
8.4.1	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
8.4.1	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
8.4.2	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
8.4.2	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
8.4.2	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
8.4.2	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.
8.4.2	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	AWS 구성 규칙	지침
8.4.2	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
8.4.2	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
8.4.2	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
8.4.2	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
8.4.2	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
8.4.2	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
8.4.4	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
8.5.4	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
8.5.4	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
9.1.1	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
9.1.1	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	AWS 구성 규칙	지침
9.1.1	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
9.1.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
9.1.1	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	AWS 구성 규칙	지침
9.1.1	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
9.1.1	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
9.1.1	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
9.1.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
9.1.1	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
9.1.1	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
9.1.1	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
9.1.1	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
9.1.1	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
9.1.1	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
9.1.1	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
9.1.1	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
9.1.1	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
9.1.1	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
9.1.1	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
9.1.1	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
9.1.1	secretsmanager-secret-periodic-rotation	이 규칙은 AWS Secrets Manager 보안 암호에 주기적 교체가 활성화되어 있도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다. 기본값은 90일입니다.

제어 ID	AWS 구성 규칙	지침
9.1.1	secretsmanager-secret-unused	AWS Secrets Manager에 미사용 자격 증명이 있는 경우 최소 권한 원칙을 위반할 수 있으므로 자격 증명을 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하면 값을 unusedForDays(Config 기본값: 90)로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
9.1.2	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
9.1.2	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
9.1.2	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
9.1.2	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
9.1.2	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
9.1.2	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
9.1.3	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
9.1.3	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
9.1.3	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
9.1.3	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
9.1.3	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
9.1.3	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail의 사용이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
9.1.3	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
9.1.3	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
9.1.3	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
9.1.3	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
9.1.3	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
9.1.3	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
9.1.3	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
9.1.3	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
9.1.3	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
9.1.3	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
9.1.3	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
9.1.3	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	AWS 구성 규칙	지침
9.1.4	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
9.1.5	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
9.1.5	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
9.1.5	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
9.1.5	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
9.1.6	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
9.1.7	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
9.1.7	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
9.1.7	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	AWS 구성 규칙	지침
9.1.7	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
9.1.7	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
9.1.7	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
9.2.1	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
9.2.1	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
9.2.1	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
9.2.1	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
9.2.1	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
9.2.1	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	AWS 구성 규칙	지침
9.2.1	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
9.2.1	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
9.2.1	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	AWS 구성 규칙	지침
9.2.1	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
9.2.1	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
9.2.2	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
9.2.2	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
9.2.2	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
9.2.2	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
9.2.2	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
9.2.2	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	AWS 구성 규칙	지침
9.2.2	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
9.2.2	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
9.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	AWS 구성 규칙	지침
9.2.2	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
9.2.2	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
9.3.1	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
9.3.1	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
9.3.1	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
9.3.1	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
9.3.1	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
9.3.1	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
9.3.1	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
9.3.1	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
9.3.1	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
9.3.1	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
9.3.1	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
9.3.1	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
9.3.1	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
9.3.1	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
9.3.1	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.1.1	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
10.1.1	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
10.1.1	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
10.1.1	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
10.1.1	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
10.1.1	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
10.1.1	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
10.1.1	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.1.1	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
10.1.1	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
10.1.1	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
10.1.1	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.1.1	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
10.1.1	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
10.1.1	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.1.1	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	AWS 구성 규칙	지침
10.1.1	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
10.1.1	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.1.1	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
10.1.1	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
10.1.1	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.1.1	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
10.1.1	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
10.1.1	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.1.1	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
10.1.1	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.1.1	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.1.1	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
10.1.1	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.2.1	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
10.2.1	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
10.2.1	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	AWS 구성 규칙	지침
10.2.2	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
10.2.3	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
10.2.3	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	AWS 구성 규칙	지침
10.2.3	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
11.1.1 (a)	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
11.1.1 (a)	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (a)	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
11.1.1 (a)	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
11.1.1 (a)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (a)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (a)	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
11.1.1 (a)	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (a)	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (a)	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (b)	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
11.1.1 (b)	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
11.1.1 (b)	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
11.1.1 (b)	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.1.1 (b)	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.1.1 (b)	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (b)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.1.1 (b)	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
11.1.1 (b)	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
11.1.1 (b)	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
11.1.1 (b)	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.1.1 (b)	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
11.1.1 (b)	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
11.1.1 (b)	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
11.1.1 (b)	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.1.1 (b)	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (b)	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (b)	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (b)	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
11.1.1 (b)	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
11.1.1 (b)	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (b)	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (b)	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (b)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (b)	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.1 (b)	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
11.1.1 (b)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
11.1.3	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
11.1.3	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
11.1.3	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
11.1.3	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
11.1.3	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.1.3	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.3	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
11.1.3	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
11.1.3	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
11.1.3	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
11.1.3	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
11.1.3	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	AWS 구성 규칙	지침
11.1.3	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
11.1.3	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	AWS 구성 규칙	지침
11.1.3	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
11.1.3	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
11.1.3	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
11.1.3	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
11.1.3	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
11.1.3	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
11.1.3	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
11.1.3	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
11.1.3	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
11.1.3	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
11.1.3	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.3	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
11.1.3	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
11.1.3	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
11.1.3	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
11.1.3	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
11.1.3	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
11.1.3	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.3	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.3	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
11.1.3	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.1.3	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
11.2.1	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
11.2.2	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
11.2.2	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.2.2	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.2.2	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
11.2.2	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
11.2.2	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	AWS 구성 규칙	지침
11.2.2	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.2.2	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
11.2.2	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
11.2.2	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
11.2.2	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
11.2.2	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
11.2.2	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
11.2.2	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.2.2	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
11.2.2	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
11.2.2	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
11.2.2	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
11.2.2	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
11.2.2	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
11.2.2	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	AWS 구성 규칙	지침
11.2.2	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
11.2.2	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
11.2.4	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
11.2.4	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.2.4	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.2.4	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
11.2.4	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.2.4	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
11.2.4	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
11.2.4	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
11.2.4	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
11.2.4	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
11.2.4	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
11.2.4	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
11.2.4	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11.2.4	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
11.2.4	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
11.2.4	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
11.2.4	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
11.2.4	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
11.2.4	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
11.2.4	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
11.2.4	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
11.3.1	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
11.3.5	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
11.3.5	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
11.3.5	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
11.3.5	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
11.4.2	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
11.4.2	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
11.4.2	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
11.4.2	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
11.5.2	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
12.1.1	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
12.1.1	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
12.1.1	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	AWS 구성 규칙	지침
12.1.1	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
12.2.2	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
12.2.2	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
12.2.2	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
12.2.2	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
12.2.2	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
12.2.2	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
12.2.2	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
12.2.2	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
12.2.2	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
12.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
12.2.2	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
12.2.2	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
12.2.2	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
12.2.2	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
12.2.2	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
12.2.2	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
12.2.4	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
12.2.4	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
12.2.5	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
12.2.5	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
12.2.5	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	AWS 구성 규칙	지침
12.2.5	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
12.3.2	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
12.3.2	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
12.3.2	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	AWS 구성 규칙	지침
14.1.2	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
14.1.2	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
14.1.2	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
14.1.2	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
14.1.2	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
14.1.2	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
14.1.2	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
14.1.2	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
14.1.2	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
14.1.3	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.
14.1.3	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
14.1.3	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
14.1.3	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
14.2.2	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
14.2.2	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
14.2.2	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
14.2.2	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
14.2.2	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
14.2.2	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
14.2.2	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
14.2.2	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
14.2.2	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
14.2.2	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
14.2.2	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	AWS 구성 규칙	지침
14.2.2	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
14.2.6	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
14.2.6	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
14.2.6	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
14.2.6	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
14.2.6	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
14.2.6	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
14.2.6	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
14.2.6	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

템플릿

템플릿은 GitHub: MAS TRMG 운영 모범 사례에서 확인할 수 있습니다.

모니터링 운영 모범 사례

이 적합성 팩에는 내부 모니터링을 기반으로 하는 AWS Config 규칙이 포함되어 있습니다 AWS. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 모니터링 운영 모범 사례에서 사용할 수 있습니다.

NBC TRMG 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙과 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 캄보디아 국립 은행(NBC)의 기술 위험 관리(TRM) 지침 프레임워크와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 NBC TRM 지침과 관련이 있습니다. NBC TRM 지침은 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 샘플 적합성 팩 템플릿에는 National Bank of Cambodia(NBC)의 기술 위험 관리(TRM) 지침 프레임워크 내의 컨트롤에 대한 매핑이 포함되어 있습니다.이 프레임워크는 National Bank of Cambodia: Technology Risk Management Guidelines에서 액세스할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능 원칙을 통합할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	[api-gw-execution-logging-enabled](#)	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자와 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS 관리 콘솔 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management(IAM) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	account-part-of-organizations	AWS Organizations AWS 계정 내의 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있도록 하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 인라인 정책 대신 관리형 정책을 사용할 것을 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹에 속하도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(d)	d) 고려해야 할 중요한 제어 항목은 다음과 같습니다. - 사용자 ID 및 액세스 제어 매트릭스 생성을 적용하고 승인하는 체계적인 프로세스 - 위험 평가를 수행하고 이에 기반한 액세스 권한 부여. - 효과적인 업무 분리를 보장하기 위해 설계된 역할 기반 액세스 제어 구현 - 시스템의 기본 사용자 이름 및/또는 암호 변경 및 일반 계정의 사용자 ID 및 암호 공유 금지 - 역할 또는 책임이 변경될 때마다 액세스 권한 수정 및 고용/계약 종료 시 액세스 권한 제거 - 정보 보안 부서에 사용자 추가, 삭제 및 역할 변경에 관해 적시에 알리는 프로세스 - 시스템 내 사용자 ID와 실제 액세스가 필요한 사용자를 주기적으로 조정하고 불필요한 ID 삭제 - 모든 사용자의 IT 자산 액세스 감사, 기록 및 모니터링 - 장기 휴가 중인 중요 애플리케이	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	션 사용자의 사용자 ID 비활성화 고려		
3.1.1(f)	f) 책임 규명을 위해 사용자와 IT 자산을 고유하게 식별하고 해당 활동을 감사할 수 있도록 해야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자와 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(f)	f) 책임 규명을 위해 사용자와 IT 자산을 고유하게 식별하고 해당 활동을 감사할 수 있도록 해야 합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS 관리 콘솔 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(f)	f) 책임 규명을 위해 사용자와 IT 자산을 고유하게 식별하고 해당 활동을 감사할 수 있도록 해야 합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
3.1.1(f)	f) 책임 규명을 위해 사용자와 IT 자산을 고유하게 식별하고 해당 활동을 감사할 수 있도록 해야 합니다.	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(f)	f) 책임 규명을 위해 사용자와 IT 자산을 고유하게 식별하고 해당 활동을 감사할 수 있도록 해야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(f)	f) 책임 규명을 위해 사용자와 IT 자산을 고유하게 식별하고 해당 활동을 감사할 수 있도록 해야 합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
3.1.1(f)	f) 책임 규명을 위해 사용자와 IT 자산을 고유하게 식별하고 해당 활동을 감사할 수 있도록 해야 합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 IAM 암호 정책에 사용합니다. 실제 값은 조

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능 원칙을 통합할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-user-no-policies-check	이 규칙은 AWS Identity and Access Management(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	[api-gw-execution-logging-enabled](#)	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자와 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS 관리 콘솔 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	account-part-of-organizations	AWS Organizations AWS 계정 내의 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있도록 하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 인라인 정책 대신 관리형 정책을 사용할 것을 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹에 속하도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 사용자가 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1(h)	h) 시스템 관리자, 보안 책임자, 프로그래머 및 중요한 작업을 수행하는 직원은 맡은 직무와 접근 권한 때문에 항상 자신이 유지 관리하거나 운영하는 재무 시스템에 심각한 피해를 입힐 수 있습니다. 시스템 액세스 권한이 높은 직원은 시스템 제어 및 보안 절차를 우회할 수 있는 내부 지식과 자원을 보유하고 있으므로 이들의 모든 시스템 활동을 기록하여 면밀히 감독해야 합니다. 아래 열거된 몇 가지 제어 및 보안 관행을 고려해야 합니다. - 권한 있는 사용자에 대한 2단계 인증 구현 - 권한 있는 사용자의 원격 액세스에 대한 강력한 제어 구현 - 권한 있는 사용자의 수 제한 - '필요' 또는 '해야 할 일'에 따라 액세스 권한 부여 - 권한 있는 사용자가 수행하는 시스템 활동에 대한 감사 로깅 유지 - 활동을 캡처 중인 동안에는 권한 있는 사용자가 시스	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	템 로그에 액세스할 수 없도록 보장 - 정기적인 로그 감사 또는 관리 검토 수행 - 권한 있는 ID 및 액세스 코드의 공유 금지 - 공급업체 및 계약업체가 면밀한 감독 및 모니터링 없이 시스템에 대한 권한 있는 액세스를 획득하는 것을 금지 - 무단 액세스로부터 백업 데이터 보호		
3.1.2(a)	a) BFI는 네트워크 경계를 보호하기 위해 IT 인프라의 중요한 지점에 방화벽, 바이러스 백신/멀웨어 방지 소프트웨어, 침입 탐지 및 방지 시스템과 같은 네트워크 보안 디바이스를 설치해야 합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(a)	a) BFI는 네트워크 경계를 보호하기 위해 IT 인프라의 중요한 지점에 방화벽, 바이러스 백신/멀웨어 방지 소프트웨어, 침입 탐지 및 방지 시스템과 같은 네트워크 보안 디바이스를 설치해야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
3.1.2(a)	a) BFI는 네트워크 경계를 보호하기 위해 IT 인프라의 중요한 지점에 방화벽, 바이러스 백신/멀웨어 방지 소프트웨어, 침입 탐지 및 방지 시스템과 같은 네트워크 보안 디바이스를 설치해야 합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration 값이 필요합니다(AWS 기본 보안 모범 사례 값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	[api-gw-execution-logging-enabled](#)	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자와 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS 관리 콘솔 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management(IAM) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 수신 및 송신 네트워크 트래픽의 상태 저장 필터링을 제공하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	lambda-inside-vpc	함수와 Amazon VPC 내 다른 서비스 간의 안전한 통신을 위해 Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lambda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	rds-instance-public-access-check	Amazon Relational Database Service(RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	rds-snapshots-public-prohibited	Amazon Relational Database Service(RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북이 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 수신 및 송신 네트워크 트래픽의 상태 저장 필터링을 제공하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(c)	c) 네트워크 내 정보의 보안을 보장하고 연결된 서비스를 무단 액세스로부터 보호하기 위한 통제책을 구현해야 합니다. 특히 다음 항목을 고려해야 합니다. - 네트워킹 장비 관리에 대한 책임 및 절차를 설정해야 합니다. - 네트워크에 대한 운영 책임은 적절한 경우 컴퓨터 운영과 분리되어야 합니다. - 공용 네트워크 또는 무선 네트워크를 통해 전달되는 데이터의 기밀성과 무결성을 보호하고 연결된 시스템 및 애플리케이션을 보호하기 위한 특수한 통제책을 수립해야 합니다(신뢰할 수 없는 시스템/네트워크에 연결할 경우 네트워크 암호화 프로토콜 포함). - 정보 보안에 영향을 미칠 수 있거나 이와 관련된 조치를 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. - 조직에 대한 서비스를 최적화하고 정보 처리 인프라 전반에	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	통제가 일관되게 적용되도록 관리 활동을 긴밀하게 조정해야 합니다. - 네트워크상의 시스템을 인증해야 합니다. - 네트워크에 대한 신뢰할 수 없는 시스템 연결을 제한해야 합니다.		
3.1.2(e)	e) 네트워크 서비스는 단순한 비관리형 대역폭부터 VPN, VoIP, VSAT 등의 정교한 서비스에 이르기까지 다양합니다. 네트워크 서비스의 보안 기능은 다음과 같아야 합니다. - 인증, 암호화 및 네트워크 연결 제어와 같은 네트워크 서비스의 보안을 위해 적용되는 기술 - 보안 및 네트워크 연결 규칙에 따라 네트워크 서비스와의 보안 연결에 필요한 기술 파라미터 - 필요한 경우 네트워크 서비스 또는 애플리케이션에 대한 액세스를 제한하기 위한 네트워크 서비스 사용 절차	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration 값이 필요합니다(AWS 기본 보안 모범 사례 값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(e)	e) 네트워크 서비스는 단순한 비관리형 대역폭부터 VPN, VoIP, VSAT 등의 정교한 서비스에 이르기까지 다양합니다. 네트워크 서비스의 보안 기능은 다음과 같아야 합니다. - 인증, 암호화 및 네트워크 연결 제어와 같은 네트워크 서비스의 보안을 위해 적용되는 기술 - 보안 및 네트워크 연결 규칙에 따라 네트워크 서비스와의 보안 연결에 필요한 기술 파라미터 - 필요한 경우 네트워크 서비스 또는 애플리케이션에 대한 액세스를 제한하기 위한 네트워크 서비스 사용 절차	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(e)	e) 네트워크 서비스는 단순한 비관리형 대역폭부터 VPN, VoIP, VSAT 등의 정교한 서비스에 이르기까지 다양합니다. 네트워크 서비스의 보안 기능은 다음과 같아야 합니다. - 인증, 암호화 및 네트워크 연결 제어와 같은 네트워크 서비스의 보안을 위해 적용되는 기술 - 보안 및 네트워크 연결 규칙에 따라 네트워크 서비스와의 보안 연결에 필요한 기술 파라미터 - 필요한 경우 네트워크 서비스 또는 애플리케이션에 대한 액세스를 제한하기 위한 네트워크 서비스 사용 절차	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(e)	e) 네트워크 서비스는 단순한 비관리형 대역폭부터 VPN, VoIP, VSAT 등의 정교한 서비스에 이르기까지 다양합니다. 네트워크 서비스의 보안 기능은 다음과 같아야 합니다. - 인증, 암호화 및 네트워크 연결 제어와 같은 네트워크 서비스의 보안을 위해 적용되는 기술 - 보안 및 네트워크 연결 규칙에 따라 네트워크 서비스와의 보안 연결에 필요한 기술 파라미터 - 필요한 경우 네트워크 서비스 또는 애플리케이션에 대한 액세스를 제한하기 위한 네트워크 서비스 사용 절차	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(e)	e) 네트워크 서비스는 단순한 비관리형 대역폭부터 VPN, VoIP, VSAT 등의 정교한 서비스에 이르기까지 다양합니다. 네트워크 서비스의 보안 기능은 다음과 같아야 합니다. - 인증, 암호화 및 네트워크 연결 제어와 같은 네트워크 서비스의 보안을 위해 적용되는 기술 - 보안 및 네트워크 연결 규칙에 따라 네트워크 서비스와의 보안 연결에 필요한 기술 파라미터 - 필요한 경우 네트워크 서비스 또는 애플리케이션에 대한 액세스를 제한하기 위한 네트워크 서비스 사용 절차	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(e)	e) 네트워크 서비스는 단순한 비관리형 대역폭부터 VPN, VoIP, VSAT 등의 정교한 서비스에 이르기까지 다양합니다. 네트워크 서비스의 보안 기능은 다음과 같아야 합니다. - 인증, 암호화 및 네트워크 연결 제어와 같은 네트워크 서비스의 보안을 위해 적용되는 기술 - 보안 및 네트워크 연결 규칙에 따라 네트워크 서비스와의 보안 연결에 필요한 기술 파라미터 - 필요한 경우 네트워크 서비스 또는 애플리케이션에 대한 액세스를 제한하기 위한 네트워크 서비스 사용 절차	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(e)	e) 네트워크 서비스는 단순한 비관리형 대역폭부터 VPN, VoIP, VSAT 등의 정교한 서비스에 이르기까지 다양합니다. 네트워크 서비스의 보안 기능은 다음과 같아야 합니다. - 인증, 암호화 및 네트워크 연결 제어와 같은 네트워크 서비스의 보안을 위해 적용되는 기술 - 보안 및 네트워크 연결 규칙에 따라 네트워크 서비스와의 보안 연결에 필요한 기술 파라미터 - 필요한 경우 네트워크 서비스 또는 애플리케이션에 대한 액세스를 제한하기 위한 네트워크 서비스 사용 절차	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(e)	e) 네트워크 서비스는 단순한 비관리형 대역폭부터 VPN, VoIP, VSAT 등의 정교한 서비스에 이르기까지 다양합니다. 네트워크 서비스의 보안 기능은 다음과 같아야 합니다. - 인증, 암호화 및 네트워크 연결 제어와 같은 네트워크 서비스의 보안을 위해 적용되는 기술 - 보안 및 네트워크 연결 규칙에 따라 네트워크 서비스와의 보안 연결에 필요한 기술 파라미터 - 필요한 경우 네트워크 서비스 또는 애플리케이션에 대한 액세스를 제한하기 위한 네트워크 서비스 사용 절차	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(e)	e) 네트워크 서비스는 단순한 비관리형 대역폭부터 VPN, VoIP, VSAT 등의 정교한 서비스에 이르기까지 다양합니다. 네트워크 서비스의 보안 기능은 다음과 같아야 합니다. - 인증, 암호화 및 네트워크 연결 제어와 같은 네트워크 서비스의 보안을 위해 적용되는 기술 - 보안 및 네트워크 연결 규칙에 따라 네트워크 서비스와의 보안 연결에 필요한 기술 파라미터 - 필요한 경우 네트워크 서비스 또는 애플리케이션에 대한 액세스를 제한하기 위한 네트워크 서비스 사용 절차	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(e)	e) 네트워크 서비스는 단순한 비관리형 대역폭부터 VPN, VoIP, VSAT 등의 정교한 서비스에 이르기까지 다양합니다. 네트워크 서비스의 보안 기능은 다음과 같아야 합니다. - 인증, 암호화 및 네트워크 연결 제어와 같은 네트워크 서비스의 보안을 위해 적용되는 기술 - 보안 및 네트워크 연결 규칙에 따라 네트워크 서비스와의 보안 연결에 필요한 기술 파라미터 - 필요한 경우 네트워크 서비스 또는 애플리케이션에 대한 액세스를 제한하기 위한 네트워크 서비스 사용 절차	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2(e)	e) 네트워크 서비스는 단순한 비관리형 대역폭부터 VPN, VoIP, VSAT 등의 정교한 서비스에 이르기까지 다양합니다. 네트워크 서비스의 보안 기능은 다음과 같아야 합니다. - 인증, 암호화 및 네트워크 연결 제어와 같은 네트워크 서비스의 보안을 위해 적용되는 기술 - 보안 및 네트워크 연결 규칙에 따라 네트워크 서비스와의 보안 연결에 필요한 기술 파라미터 - 필요한 경우 네트워크 서비스 또는 애플리케이션에 대한 액세스를 제한하기 위한 네트워크 서비스 사용 절차	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(e)	e) 암호화를 사용하여 원격 액세스 디바이스와 기관 간의 통신 채널을 보호하여 네트워크 스푸핑과 관련된 위험을 제한합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration 값이 필요합니다(AWS 기본 보안 모범 사례 값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
3.1.3(e)	e) 암호화를 사용하여 원격 액세스 디바이스와 기관 간의 통신 채널을 보호하여 네트워크 스푸핑과 관련된 위험을 제한합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(e)	e) 암호화를 사용하여 원격 액세스 디바이스와 기관 간의 통신 채널을 보호하여 네트워크 스푸핑과 관련된 위험을 제한합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포할 수 있습니다.
3.1.3(e)	e) 암호화를 사용하여 원격 액세스 디바이스와 기관 간의 통신 채널을 보호하여 네트워크 스푸핑과 관련된 위험을 제한합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(e)	e) 암호화를 사용하여 원격 액세스 디바이스와 기관 간의 통신 채널을 보호하여 네트워크 스푸핑과 관련된 위험을 제한합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.3(e)	e) 암호화를 사용하여 원격 액세스 디바이스와 기관 간의 통신 채널을 보호하여 네트워크 스푸핑과 관련된 위험을 제한합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(e)	e) 암호화를 사용하여 원격 액세스 디바이스와 기관 간의 통신 채널을 보호하여 네트워크 스푸핑과 관련된 위험을 제한합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.3(e)	e) 암호화를 사용하여 원격 액세스 디바이스와 기관 간의 통신 채널을 보호하여 네트워크 스푸핑과 관련된 위험을 제한합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(e)	e) 암호화를 사용하여 원격 액세스 디바이스와 기관 간의 통신 채널을 보호하여 네트워크 스푸핑과 관련된 위험을 제한합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.3(e)	e) 암호화를 사용하여 원격 액세스 디바이스와 기관 간의 통신 채널을 보호하여 네트워크 스푸핑과 관련된 위험을 제한합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
3.1.3(e)	e) 암호화를 사용하여 원격 액세스 디바이스와 기관 간의 통신 채널을 보호하여 네트워크 스푸핑과 관련된 위험을 제한합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자와 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS 관리 콘솔 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
3.1.3(g)	g) 원격 액세스 통신을 위한 로그를 유지합니다. 로그에는 원격 액세스를 통해 수행된 모든 활동을 포함하여 모든 원격 액세스의 날짜, 시간, 사용자, 사용자 위치, 기간 및 목적이 포함되어야 합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(i)	i) 원격 액세스를 위한 2단계 인증 프로세스 적용(예: 일회용 무작위 암호 생성기가 있는 PIN 기반 토큰 카드 또는 토큰 기반 PKI)	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
3.1.3(i)	i) 원격 액세스를 위한 2단계 인증 프로세스 적용(예: 일회용 무작위 암호 생성기가 있는 PIN 기반 토큰 카드 또는 토큰 기반 PKI)	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3(i)	i) 원격 액세스를 위한 2단계 인증 프로세스 적용(예: 일회용 무작위 암호 생성기가 있는 PIN 기반 토큰 카드 또는 토큰 기반 PKI)	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
3.1.3(i)	i) 원격 액세스를 위한 2단계 인증 프로세스 적용(예: 일회용 무작위 암호 생성기가 있는 PIN 기반 토큰 카드 또는 토큰 기반 PKI)	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4(c)(e)	c) 패치 관리 프로세스에는 다음과 같은 측면이 포함되어야 합니다. - 패치를 승인된 출처에서 입수하기 위해 패치를 조달하고 검증하는 방법 결정 - 조직에서 사용하는 애플리케이션 및 시스템에 적용되는 취약성 식별 - 패치 구현(또는 특정 패치 구현하지 않음)이 비즈니스에 미치는 영향 평가 - 패치가 테스트되도록 보장 - 패치 배포 방법 설명(예: 자동) - 조직 전반의 패치 배포 상태에 대한 보고 - 패치 배포 실패를 처리할 방법 포함(예: 패치 재배포) e) BFI는 해당 도구를 사용할 수 있고 안전한 모든 시스템에 자동화된 패치 관리 도구 및 소프트웨어 업데이트 도구를 배포해야 합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 자세한 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4(c)(e)	c) 패치 관리 프로세스에는 다음과 같은 측면이 포함되어야 합니다. - 패치를 승인된 출처에서 입수하기 위해 패치를 조달하고 검증하는 방법 결정 - 조직에서 사용하는 애플리케이션 및 시스템에 적용되는 취약성 식별 - 패치 구현(또는 특정 패치 구현하지 않음)이 비즈니스에 미치는 영향 평가 - 패치가 테스트되도록 보장 - 패치 배포 방법 설명(예: 자동) - 조직 전반의 패치 배포 상태에 대한 보고 - 패치 배포 실패를 처리할 방법 포함(예: 패치 재배포) e) BFI는 해당 도구를 사용할 수 있고 안전한 모든 시스템에 자동화된 패치 관리 도구 및 소프트웨어 업데이트 도구를 배포해야 합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 대한 기타 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4(c)(e)	c) 패치 관리 프로세스에는 다음과 같은 측면이 포함되어야 합니다. - 패치를 승인된 출처에서 입수하기 위해 패치를 조달하고 검증하는 방법 결정 - 조직에서 사용하는 애플리케이션 및 시스템에 적용되는 취약성 식별 - 패치 구현(또는 특정 패치 구현하지 않음)이 비즈니스에 미치는 영향 평가 - 패치가 테스트되도록 보장 - 패치 배포 방법 설명(예: 자동) - 조직 전반의 패치 배포 상태에 대한 보고 - 패치 배포 실패를 처리할 방법 포함(예: 패치 재배포) e) BFI는 해당 도구를 사용할 수 있고 안전한 모든 시스템에 자동화된 패치 관리 도구 및 소프트웨어 업데이트 도구를 배포해야 합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 이 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4(c)(e)	c) 패치 관리 프로세스에는 다음과 같은 측면이 포함되어야 합니다. - 패치를 승인된 출처에서 입수하기 위해 패치를 조달하고 검증하는 방법 결정 - 조직에서 사용하는 애플리케이션 및 시스템에 적용되는 취약성 식별 - 패치 구현(또는 특정 패치 구현하지 않음)이 비즈니스에 미치는 영향 평가 - 패치가 테스트되도록 보장 - 패치 배포 방법 설명(예: 자동) - 조직 전반의 패치 배포 상태에 대한 보고 - 패치 배포 실패를 처리할 방법 포함(예: 패치 재배포) e) BFI는 해당 도구를 사용할 수 있고 안전한 모든 시스템에 자동화된 패치 관리 도구 및 소프트웨어 업데이트 도구를 배포해야 합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4(c)(e)	c) 패치 관리 프로세스에는 다음과 같은 측면이 포함되어야 합니다. - 패치를 승인된 출처에서 입수하기 위해 패치를 조달하고 검증하는 방법 결정 - 조직에서 사용하는 애플리케이션 및 시스템에 적용되는 취약성 식별 - 패치 구현(또는 특정 패치 구현하지 않음)이 비즈니스에 미치는 영향 평가 - 패치가 테스트되도록 보장 - 패치 배포 방법 설명(예: 자동) - 조직 전반의 패치 배포 상태에 대한 보고 - 패치 배포 실패를 처리할 방법 포함(예: 패치 재배포) e) BFI는 해당 도구를 사용할 수 있고 안전한 모든 시스템에 자동화된 패치 관리 도구 및 소프트웨어 업데이트 도구를 배포해야 합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4(c)(e)	c) 패치 관리 프로세스에는 다음과 같은 측면이 포함되어야 합니다. - 패치를 승인된 출처에서 입수하기 위해 패치를 조달하고 검증하는 방법 결정 - 조직에서 사용하는 애플리케이션 및 시스템에 적용되는 취약성 식별 - 패치 구현(또는 특정 패치 구현하지 않음)이 비즈니스에 미치는 영향 평가 - 패치가 테스트되도록 보장 - 패치 배포 방법 설명(예: 자동) - 조직 전반의 패치 배포 상태에 대한 보고 - 패치 배포 실패를 처리할 방법 포함(예: 패치 재배포) e) BFI는 해당 도구를 사용할 수 있고 안전한 모든 시스템에 자동화된 패치 관리 도구 및 소프트웨어 업데이트 도구를 배포해야 합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5(d)(e)	d) 적절한 키 관리를 위해서는 암호화 키의 생성, 저장, 보관, 검색, 배포, 사용 중지 및 폐기를 위한 안전한 프로세스가 필요합니다. e) 모든 암호화 키는 수정 및 손실로부터 보호되어야 합니다. 또한 비밀 키와 개인 키의 무단 사용 및 공개를 방지해야 합니다. 키를 생성, 저장 및 보관하는 데 사용되는 장비는 물리적으로 보호되어야 합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
3.1.5(d)(e)	d) 적절한 키 관리를 위해서는 암호화 키의 생성, 저장, 보관, 검색, 배포, 사용 중지 및 폐기를 위한 안전한 프로세스가 필요합니다. e) 모든 암호화 키는 수정 및 손실로부터 보호되어야 합니다. 또한 비밀 키와 개인 키의 무단 사용 및 공개를 방지해야 합니다. 키를 생성, 저장 및 보관하는 데 사용되는 장비는 물리적으로 보호되어야 합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5(d)(e)	d) 적절한 키 관리를 위해서는 암호화 키의 생성, 저장, 보관, 검색, 배포, 사용 중지 및 폐기를 위한 안전한 프로세스가 필요합니다. e) 모든 암호화 키는 수정 및 손실로부터 보호되어야 합니다. 또한 비밀 키와 개인 키의 무단 사용 및 공개를 방지해야 합니다. 키를 생성, 저장 및 보관하는 데 사용되는 장비는 물리적으로 보호되어야 합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5(d)(e)	d) 적절한 키 관리를 위해서는 암호화 키의 생성, 저장, 보관, 검색, 배포, 사용 중지 및 폐기를 위한 안전한 프로세스가 필요합니다. e) 모든 암호화 키는 수정 및 손실로부터 보호되어야 합니다. 또한 비밀 키와 개인 키의 무단 사용 및 공개를 방지해야 합니다. 키를 생성, 저장 및 보관하는 데 사용되는 장비는 물리적으로 보호되어야 합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 인라인 정책 대신 관리형 정책을 사용할 것을 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5(f)	f) 키 관리 시스템은 다음을 위해 합의된 표준, 절차 및 보안 방법을 기반으로 해야 합니다. - 다양한 암호화 시스템 및 애플리케이션에 대한 키 생성 - 공개 키 인증서 발급 및 획득 - 키를 수신했을 때 활성화하는 방법을 포함하여 의도한 엔터티에 키 배포 - 승인된 사용자가 키에 액세스하는 방법을 포함한 키 저장 - 키 변경 시기 및 변경 방법에 대한 규칙을 포함한 키 변경 또는 업데이트 - 손상된 키 처리 - 키가 손상되었거나 사용자의 퇴사(이 경우 키 보관도 필요) 등의 상황에서 키를 철회하거나 비활성화하는 방법을 포함한 키 취소 - 분실 또는 손상된 키 복구 - 키 백업 또는 보관 - 키 파기, - 키 관리 관련 활동의 로깅 및 감사	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5(f)	f) 키 관리 시스템은 다음을 위해 합의된 표준, 절차 및 보안 방법을 기반으로 해야 합니다. - 다양한 암호화 시스템 및 애플리케이션에 대한 키 생성 - 공개 키 인증서 발급 및 획득 - 키를 수신했을 때 활성화하는 방법을 포함하여 의도한 엔터티에 키 배포 - 승인된 사용자가 키에 액세스하는 방법을 포함한 키 저장 - 키 변경 시기 및 변경 방법에 대한 규칙을 포함한 키 변경 또는 업데이트 - 손상된 키 처리 - 키가 손상되었거나 사용자의 퇴사(이 경우 키 보관도 필요) 등의 상황에서 키를 철회하거나 비활성화하는 방법을 포함한 키 취소 - 분실 또는 손상된 키 복구 - 키 백업 또는 보관 - 키 파기, - 키 관리 관련 활동의 로깅 및 감사	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5(f)	f) 키 관리 시스템은 다음을 위해 합의된 표준, 절차 및 보안 방법을 기반으로 해야 합니다. - 다양한 암호화 시스템 및 애플리케이션에 대한 키 생성 - 공개 키 인증서 발급 및 획득 - 키를 수신했을 때 활성화하는 방법을 포함하여 의도한 엔터티에 키 배포 - 승인된 사용자가 키에 액세스하는 방법을 포함한 키 저장 - 키 변경 시기 및 변경 방법에 대한 규칙을 포함한 키 변경 또는 업데이트 - 손상된 키 처리 - 키가 손상되었거나 사용자의 퇴사(이 경우 키 보관도 필요) 등의 상황에서 키를 철회하거나 비활성화하는 방법을 포함한 키 취소 - 분실 또는 손상된 키 복구 - 키 백업 또는 보관 - 키 파기, - 키 관리 관련 활동의 로깅 및 감사	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration 값이 필요합니다(AWS 기본 보안 모범 사례 값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5(f)	f) 키 관리 시스템은 다음을 위해 합의된 표준, 절차 및 보안 방법을 기반으로 해야 합니다. - 다양한 암호화 시스템 및 애플리케이션에 대한 키 생성 - 공개 키 인증서 발급 및 획득 - 키를 수신했을 때 활성화하는 방법을 포함하여 의도한 엔터티에 키 배포 - 승인된 사용자가 키에 액세스하는 방법을 포함한 키 저장 - 키 변경 시기 및 변경 방법에 대한 규칙을 포함한 키 변경 또는 업데이트 - 손상된 키 처리 - 키가 손상되었거나 사용자의 퇴사(이 경우 키 보관도 필요) 등의 상황에서 키를 철회하거나 비활성화하는 방법을 포함한 키 취소 - 분실 또는 손상된 키 복구 - 키 백업 또는 보관 - 키 파기, - 키 관리 관련 활동의 로깅 및 감사	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5(f)	f) 키 관리 시스템은 다음을 위해 합의된 표준, 절차 및 보안 방법을 기반으로 해야 합니다. - 다양한 암호화 시스템 및 애플리케이션에 대한 키 생성 - 공개 키 인증서 발급 및 획득 - 키를 수신했을 때 활성화하는 방법을 포함하여 의도한 엔터티에 키 배포 - 승인된 사용자가 키에 액세스하는 방법을 포함한 키 저장 - 키 변경 시기 및 변경 방법에 대한 규칙을 포함한 키 변경 또는 업데이트 - 손상된 키 처리 - 키가 손상되었거나 사용자의 퇴사(이 경우 키 보관도 필요) 등의 상황에서 키를 철회하거나 비활성화하는 방법을 포함한 키 취소 - 분실 또는 손상된 키 복구 - 키 백업 또는 보관 - 키 파기, - 키 관리 관련 활동의 로깅 및 감사	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자와 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5(f)	f) 키 관리 시스템은 다음을 위해 합의된 표준, 절차 및 보안 방법을 기반으로 해야 합니다. - 다양한 암호화 시스템 및 애플리케이션에 대한 키 생성 - 공개 키 인증서 발급 및 획득 - 키를 수신했을 때 활성화하는 방법을 포함하여 의도한 엔터티에 키 배포 - 승인된 사용자가 키에 액세스하는 방법을 포함한 키 저장 - 키 변경 시기 및 변경 방법에 대한 규칙을 포함한 키 변경 또는 업데이트 - 손상된 키 처리 - 키가 손상되었거나 사용자의 퇴사(이 경우 키 보관도 필요) 등의 상황에서 키를 철회하거나 비활성화하는 방법을 포함한 키 취소 - 분실 또는 손상된 키 복구 - 키 백업 또는 보관 - 키 파기, - 키 관리 관련 활동의 로깅 및 감사	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS 관리 콘솔 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5(f)	f) 키 관리 시스템은 다음을 위해 합의된 표준, 절차 및 보안 방법을 기반으로 해야 합니다. - 다양한 암호화 시스템 및 애플리케이션에 대한 키 생성 - 공개 키 인증서 발급 및 획득 - 키를 수신했을 때 활성화하는 방법을 포함하여 의도한 엔터티에 키 배포 - 승인된 사용자가 키에 액세스하는 방법을 포함한 키 저장 - 키 변경 시기 및 변경 방법에 대한 규칙을 포함한 키 변경 또는 업데이트 - 손상된 키 처리 - 키가 손상되었거나 사용자의 퇴사(이 경우 키 보관도 필요) 등의 상황에서 키를 철회하거나 비활성화하는 방법을 포함한 키 취소 - 분실 또는 손상된 키 복구 - 키 백업 또는 보관 - 키 파기, - 키 관리 관련 활동의 로깅 및 감사	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.6(a)	a) BFI는 정기적으로 포괄적인 VA를 수행할 수 있도록 자동화된 도구와 수동 기술을 조합하여 배포해야 합니다. 웹 기반 외부 대면 시스템의 경우 VA 범위에는 SQL 명령어 삽입 및 교차 사이트 스크립팅과 같은 일반적인 웹 취약성이 포함되어야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
3.1.6(a)	a) BFI는 정기적으로 포괄적인 VA를 수행할 수 있도록 자동화된 도구와 수동 기술을 조합하여 배포해야 합니다. 웹 기반 외부 대면 시스템의 경우 VA 범위에는 SQL 명령어 삽입 및 교차 사이트 스크립팅과 같은 일반적인 웹 취약성이 포함되어야 합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.6(a)	a) BFI는 정기적으로 포괄적인 VA를 수행할 수 있도록 자동화된 도구와 수동 기술을 조합하여 배포해야 합니다. 웹 기반 외부 대면 시스템의 경우 VA 범위에는 SQL 명령어 삽입 및 교차 사이트 스크립팅과 같은 일반적인 웹 취약성이 포함되어야 합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
3.1.6(c)	c) BFI는 VA 및 PT에서 식별된 문제를 해결하기 위한 프로세스를 수립하고 이후 수정 조치를 재검증하여 격차가 완전히 해결되었는지 확인해야 합니다.	vuln-mitigated-accepted(프로세스 확인)	새로 식별된 취약성이 교정되거나 허용된 위험으로 문서화되는지 확인합니다. 취약성은 조직의 규정 준수 요구사항에 따라 교정하거나 허용된 위험으로 처리해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.6(f)	f) 보안 부서는 부서/팀별로 아직 완화되지 않은 심각한 취약점의 수에 관한 상태 업데이트와 완화 계획을 정기적으로 고위 경영진에게 제공해야 합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
3.1.8	사용자 교육 및 인식	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지하세요. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하려면 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하려면 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.10(b)	b) 시스템 문서, 애플리케이션 소스 코드, 프로덕션 트랜잭션 데이터와 같은 민감한 정보에는 변경을 방지하기 위한 좀 더 광범위한 제어 조치가 있어야 합니다(예: 무결성 검사기, 암호화 해시). 또한 정책은 해당 정보가 포함된 인쇄물을 포함하여 민감한 정보의 배포를 최소화해야 합니다.	secretsmanager-using-cmk	저장 데이터를 보호하려면 AWS Secrets Manager 보안 암호에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.2.1(h)	h) 변경과 관련된 위험을 최소화하기 위해 BFI는 변경 전에 영향을 받는 시스템 또는 애플리케이션을 백업해야 합니다. BFI는 배포 중 또는 배포 후에 문제가 발생할 경우 이전 버전의 시스템 또는 애플리케이션으로 되돌릴 수 있는 롤백 계획을 수립해야 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(h)	h) 변경과 관련된 위험을 최소화하기 위해 BFI는 변경 전에 영향을 받는 시스템 또는 애플리케이션을 백업해야 합니다. BFI는 배포 중 또는 배포 후에 문제가 발생할 경우 이전 버전의 시스템 또는 애플리케이션으로 되돌릴 수 있는 롤백 계획을 수립해야 합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
3.2.1(h)	h) 변경과 관련된 위험을 최소화하기 위해 BFI는 변경 전에 영향을 받는 시스템 또는 애플리케이션을 백업해야 합니다. BFI는 배포 중 또는 배포 후에 문제가 발생할 경우 이전 버전의 시스템 또는 애플리케이션으로 되돌릴 수 있는 롤백 계획을 수립해야 합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(h)	h) 변경과 관련된 위험을 최소화하기 위해 BFI는 변경 전에 영향을 받는 시스템 또는 애플리케이션을 백업해야 합니다. BFI는 배포 중 또는 배포 후에 문제가 발생할 경우 이전 버전의 시스템 또는 애플리케이션으로 되돌릴 수 있는 롤백 계획을 수립해야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
3.2.1(h)	h) 변경과 관련된 위험을 최소화하기 위해 BFI는 변경 전에 영향을 받는 시스템 또는 애플리케이션을 백업해야 합니다. BFI는 배포 중 또는 배포 후에 문제가 발생할 경우 이전 버전의 시스템 또는 애플리케이션으로 되돌릴 수 있는 롤백 계획을 수립해야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(h)	h) 변경과 관련된 위험을 최소화하기 위해 BFI는 변경 전에 영향을 받는 시스템 또는 애플리케이션을 백업해야 합니다. BFI는 배포 중 또는 배포 후에 문제가 발생할 경우 이전 버전의 시스템 또는 애플리케이션으로 되돌릴 수 있는 롤백 계획을 수립해야 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
3.2.1(h)	h) 변경과 관련된 위험을 최소화하기 위해 BFI는 변경 전에 영향을 받는 시스템 또는 애플리케이션을 백업해야 합니다. BFI는 배포 중 또는 배포 후에 문제가 발생할 경우 이전 버전의 시스템 또는 애플리케이션으로 되돌릴 수 있는 롤백 계획을 수립해야 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스를 지원하려면 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(h)	h) 변경과 관련된 위험을 최소화하기 위해 BFI는 변경 전에 영향을 받는 시스템 또는 애플리케이션을 백업해야 합니다. BFI는 배포 중 또는 배포 후에 문제가 발생할 경우 이전 버전의 시스템 또는 애플리케이션으로 되돌릴 수 있는 롤백 계획을 수립해야 합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
3.2.1(h)	h) 변경과 관련된 위험을 최소화하기 위해 BFI는 변경 전에 영향을 받는 시스템 또는 애플리케이션을 백업해야 합니다. BFI는 배포 중 또는 배포 후에 문제가 발생할 경우 이전 버전의 시스템 또는 애플리케이션으로 되돌릴 수 있는 롤백 계획을 수립해야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(h)	h) 변경과 관련된 위험을 최소화하기 위해 BFI는 변경 전에 영향을 받는 시스템 또는 애플리케이션을 백업해야 합니다. BFI는 배포 중 또는 배포 후에 문제가 발생할 경우 이전 버전의 시스템 또는 애플리케이션으로 되돌릴 수 있는 롤백 계획을 수립해야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
3.2.1(h)	h) 변경과 관련된 위험을 최소화하기 위해 BFI는 변경 전에 영향을 받는 시스템 또는 애플리케이션을 백업해야 합니다. BFI는 배포 중 또는 배포 후에 문제가 발생할 경우 이전 버전의 시스템 또는 애플리케이션으로 되돌릴 수 있는 롤백 계획을 수립해야 합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자와 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS 관리 콘솔 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
3.2.1(k)	k) 감사 및 보안 로그는 조사 및 문제 해결을 용이하게 하는 유용한 정보입니다. BFI는 로깅 시설이 마이그레이션 프로세스 중에 수행된 활동을 기록할 수 있도록 해야 합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.3(a)	a) 정보 보안 인시던트를 예방, 탐지, 분석 및 대응하기 위한 프로세스를 개발하고 구현합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.3(a)	a) 정보 보안 인시던트를 예방, 탐지, 분석 및 대응하기 위한 프로세스를 개발하고 구현합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management(IAM) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1(a)	a) 시스템 설계의 일환으로 높은 시스템 가용성, 적절한 용량, 안정적인 성능, 빠른 응답 시간, 확장성을 유지하는 것과 관련된 중요한 요소를 고려합니다.	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자와 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS 관리 콘솔 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보, 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(a)(b)(c)(f)(j)	a) 감사 및 검토 목적으로 사용자 액세스 기록이 고유하게 식별되고 기록되도록 보장합니다. b) 무단 액세스에 대한 책임 및 식별이 문서화됩니다. c) 권한 있는 사용자가 수행한 시스템 활동에 대한 감사 로깅을 활성화합니다. f) 정보 보안에 영향을 미칠 수 있거나 관련된 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다. j) 이벤트 로깅이 시스템 보안에 대한 통합 보고서 및 경고를 생성할 수 있는 자동화된 모니터링 시스템의 기반을 설정하도록 합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(f)	f) 정보 보안에 영향을 미칠 수 있거나 관련 있는 작업을 기록하고 탐지할 수 있도록 적절한 로깅 및 모니터링을 적용해야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management(IAM) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS 관리 콘솔 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보, 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	[api-gw-execution-logging-enabled](#)	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자와 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4(g)	g) 이벤트 로그에 해당하는 경우 다음이 포함되는지 확인합니다. - 사용자 ID - 시스템 활동 - 로그온 및 로그오프와 같은 주요 이벤트의 날짜, 시간 및 세부 정보 - 가능한 경우 디바이스 ID 또는 위치 및 시스템 식별자 - 성공 및 거부된 시스템 액세스 시도 기록 - 성공 및 거부된 데이터 및 기타 리소스 액세스 시도 기록 - 시스템 구성 변경 - 권한 사용 - 시스템 유틸리티 및 애플리케이션 사용 - 액세스한 파일 및 액세스 종류 - 네트워크 주소 및 프로토콜 - 출입 통제 시스템에서 발생하는 경보 -애플리케이션 및 온라인 고객 거래에서 사용자가 실행한 거래 기록	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1(a)(h)	a) BFI는 웹 애플리케이션에 적합한 보안 조치를 취하고 다양한 웹 보안 위험에 대해 합리적인 완화 조치를 취해야 합니다. h) BFI는 웹 애플리케이션에 적합한 보안 조치를 보장하고 다양한 웹 보안 위험에 대해 합리적인 완화 조치를 취해야 합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 소비할 수 있습니다.
3.6.1(a)(h)	a) BFI는 웹 애플리케이션에 적합한 보안 조치를 취하고 다양한 웹 보안 위험에 대해 합리적인 완화 조치를 취해야 합니다. h) BFI는 웹 애플리케이션에 적합한 보안 조치를 보장하고 다양한 웹 보안 위험에 대해 합리적인 완화 조치를 취해야 합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1(b)	b) BFI는 인터넷 뱅킹 시스템 및 기타 관련 시스템과 관련된 보안 요구 사항을 평가하고 필요한 기밀성 및 무결성 정도를 고려하여 암호화 솔루션을 채택해야 합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration 값이 필요합니다(AWS 기본 보안 모범 사례 값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
3.6.1(b)	b) BFI는 인터넷 뱅킹 시스템 및 기타 관련 시스템과 관련된 보안 요구 사항을 평가하고 필요한 기밀성 및 무결성 정도를 고려하여 암호화 솔루션을 채택해야 합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1(b)	b) BFI는 인터넷 뱅킹 시스템 및 기타 관련 시스템과 관련된 보안 요구 사항을 평가하고 필요한 기밀성 및 무결성 정도를 고려하여 암호화 솔루션을 채택해야 합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
3.6.1(b)	b) BFI는 인터넷 뱅킹 시스템 및 기타 관련 시스템과 관련된 보안 요구 사항을 평가하고 필요한 기밀성 및 무결성 정도를 고려하여 암호화 솔루션을 채택해야 합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1(b)	b) BFI는 인터넷 뱅킹 시스템 및 기타 관련 시스템과 관련된 보안 요구 사항을 평가하고 필요한 기밀성 및 무결성 정도를 고려하여 암호화 솔루션을 채택해야 합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.6.1(b)	b) BFI는 인터넷 뱅킹 시스템 및 기타 관련 시스템과 관련된 보안 요구 사항을 평가하고 필요한 기밀성 및 무결성 정도를 고려하여 암호화 솔루션을 채택해야 합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1(b)	b) BFI는 인터넷 뱅킹 시스템 및 기타 관련 시스템과 관련된 보안 요구 사항을 평가하고 필요한 기밀성 및 무결성 정도를 고려하여 암호화 솔루션을 채택해야 합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.6.1(b)	b) BFI는 인터넷 뱅킹 시스템 및 기타 관련 시스템과 관련된 보안 요구 사항을 평가하고 필요한 기밀성 및 무결성 정도를 고려하여 암호화 솔루션을 채택해야 합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1(b)	b) BFI는 인터넷 뱅킹 시스템 및 기타 관련 시스템과 관련된 보안 요구 사항을 평가하고 필요한 기밀성 및 무결성 정도를 고려하여 암호화 솔루션을 채택해야 합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.6.1(b)	b) BFI는 인터넷 뱅킹 시스템 및 기타 관련 시스템과 관련된 보안 요구 사항을 평가하고 필요한 기밀성 및 무결성 정도를 고려하여 암호화 솔루션을 채택해야 합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
3.6.1(b)	b) BFI는 인터넷 뱅킹 시스템 및 기타 관련 시스템과 관련된 보안 요구 사항을 평가하고 필요한 기밀성 및 무결성 정도를 고려하여 암호화 솔루션을 채택해야 합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1(d)	d) 인터넷 뱅킹을 제공하는 BFI는 DDoS 공격의 징후가 될 수 있는 비정상적인 네트워크 트래픽 상황/시스템 성능 및 시스템 리소스 사용률의 급격한 증가에 대응해야 합니다. 따라서 모든 선제 조치와 사후 조치의 성공 여부는 네트워크와 시스템의 이상 현상을 효과적으로 감지, 모니터링 및 분석할 수 있는 적절한 도구의 배포에 달려 있습니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 소비할 수 있습니다.
3.6.1(d)	d) 인터넷 뱅킹을 제공하는 BFI는 DDoS 공격의 징후가 될 수 있는 비정상적인 네트워크 트래픽 상황/시스템 성능 및 시스템 리소스 사용률의 급격한 증가에 대응해야 합니다. 따라서 모든 선제 조치와 사후 조치의 성공 여부는 네트워크와 시스템의 이상 현상을 효과적으로 감지, 모니터링 및 분석할 수 있는 적절한 도구의 배포에 달려 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1(d)	d) 인터넷 뱅킹을 제공하는 BFI는 DDoS 공격의 징후가 될 수 있는 비정상적인 네트워크 트래픽 상황/시스템 성능 및 시스템 리소스 사용률의 급격한 증가에 대응해야 합니다. 따라서 모든 선제 조치와 사후 조치의 성공 여부는 네트워크와 시스템의 이상 현상을 효과적으로 감지, 모니터링 및 분석할 수 있는 적절한 도구의 배포에 달려 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management(IAM) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1(d)	d) 인터넷 뱅킹을 제공하는 BFI는 DDoS 공격의 징후가 될 수 있는 비정상적인 네트워크 트래픽 상황/시스템 성능 및 시스템 리소스 사용률의 급격한 증가에 대응해야 합니다. 따라서 모든 선제 조치와 사후 조치의 성공 여부는 네트워크와 시스템의 이상 현상을 효과적으로 감지, 모니터링 및 분석할 수 있는 적절한 도구의 배포에 달려 있습니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보, 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
3.6.1(d)	d) 인터넷 뱅킹을 제공하는 BFI는 DDoS 공격의 징후가 될 수 있는 비정상적인 네트워크 트래픽 상황/시스템 성능 및 시스템 리소스 사용률의 급격한 증가에 대응해야 합니다. 따라서 모든 선제 조치와 사후 조치의 성공 여부는 네트워크와 시스템의 이상 현상을 효과적으로 감지, 모니터링 및 분석할 수 있는 적절한 도구의 배포에 달려 있습니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1(e)	e) BFI는 정기적으로 정보 보안 취약성을 평가하고 기존 IT 보안 위험 관리 프레임워크의 효과를 평가하여 새로운 취약성이 적시에 해결되도록 필요한 조정을 해야 합니다. 또한 이 평가는 중대한 변경의 일환으로 수행되어야 합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 수신 및 송신 네트워크 트래픽의 상태 저장 필터링을 제공하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	lambda-inside-vpc	함수와 Amazon VPC 내 다른 서비스 간의 안전한 통신을 위해 Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lambda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	rds-instance-public-access-check	Amazon Relational Database Service(RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북이 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 수신 및 송신 네트워크 트래픽의 상태 저장 필터링을 제공하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4(a)(b)	a) 인터넷 액세스를 제한하고 중요 시스템을 일반 IT 환경과 분리합니다. b) 공격 표면 및 취약성을 줄입니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

템플릿

템플릿은 GitHub: NBC TRMG 운영 모범 사례에서 확인할 수 있습니다.

NERC CIP BCSI 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 BES 사이버 시스템 정보(BCSI), CIP-004-7 및 CIP-011-3에 대한 북미 전기 신뢰성 기업 중요 인프라 보호 표준(NERC CIP)과 AWS Config 관리형 규칙 간의 샘플 매핑을 제공합니다. 각 AWS Config 규칙은 특정 AWS 리소스에 적용되며 BCSI에 적용되는 하나 이상의 NERC CIP 제어와 관련이 있습니다. NERC CIP 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-004-7-R6-Part 6.1	각 책임 주체는 CIP-004-7 표 R6. BES 사이버 시스템 정보에	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어

제어 ID	제어 설명	AWS Config 규칙	지침
	대한 액세스 관리에 명시된 '해당 시스템'에 명시된 '해당 시스템'과 관련하여 BCSI에 대한 프로비저닝된 액세스를 승인, 확인 및 취소하기 위해 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 해당하는 각 요구 사항 부분을 모두 포함하는 하나 이상의 문서화된 액세스 관리 프로그램을 구현해야 합니다. 이 요구 사항의 맥락에서 BCSI에 대한 액세스 권한으로 간주되려면 개인은 BCSI를 획득하고 사용할 수 있는 능력을 모두 갖추고 있어야 합니다. 프로비저닝된 액세스는 개인에게 BCSI 액세스 수단(예: 물리적 키 또는 액세스 카드, 사용자 및 관련 권리/권한, 암호화 키)을 제공하기 위해 취해진 특정 조치의 결과로 간주됩니다. 섹션 6.1: CIP 예외적 상황을 제외하고 책임 주체가 결정한 바에 따라 프로비저닝 전에 필요에 따라 권한을 부여합니다(섹		가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch 대시보드 멀티테넌시 지원, OpenSearch 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	션 4.1에 따라 이미 승인된 경우 제외). 전자 BCSI에 대한 프로비저닝된 전자 액세스		

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-004-7-R6-Part 6.1	각 책임 주체는 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 명시된 '해당 시스템'에 명시된 '해당 시스템'과 관련하여 BCSI에 대한 프로비저닝된 액세스를 승인, 확인 및 취소하기 위해 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 해당하는 각 요구 사항 부분을 모두 포함하는 하나 이상의 문서화된 액세스 관리 프로그램을 구현해야 합니다. 이 요구 사항의 맥락에서 BCSI에 대한 액세스 권한으로 간주되려면 개인은 BCSI를 획득하고 사용할 수 있는 능력을 모두 갖추고 있어야 합니다. 프로비저닝된 액세스는 개인에게 BCSI 액세스 수단(예: 물리적 키 또는 액세스 카드, 사용자 및 관련 권리/권한, 암호화 키)을 제공하기 위해 취해진 특정 조치의 결과로 간주됩니다. 섹션 6.1: CIP 예외적 상황을 제	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	외하고 책임 주체가 결정한 바에 따라 프로비저닝 전에 필요에 따라 권한을 부여합니다(섹션 4.1에 따라 이미 승인된 경우 제외). 전자 BCSI에 대한 프로비저닝된 전자 액세스		

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-004-7-R6-Part 6.1	각 책임 주체는 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 명시된 '해당 시스템'에 명시된 '해당 시스템'과 관련하여 BCSI에 대한 프로비저닝된 액세스를 승인, 확인 및 취소하기 위해 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 해당하는 각 요구 사항 부분을 모두 포함하는 하나 이상의 문서화된 액세스 관리 프로그램을 구현해야 합니다. 이 요구 사항의 맥락에서 BCSI에 대한 액세스 권한으로 간주되려면 개인은 BCSI를 획득하고 사용할 수 있는 능력을 모두 갖추고 있어야 합니다. 프로비저닝된 액세스는 개인에게 BCSI 액세스 수단(예: 물리적 키 또는 액세스 카드, 사용자 및 관련 권리/권한, 암호화 키)을 제공하기 위해 취해진 특정 조치의 결과로 간주됩니다. 섹션 6.1: CIP 예외적 상황을 제	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	외하고 책임 주체가 결정한 바에 따라 프로비저닝 전에 필요에 따라 권한을 부여합니다(섹션 4.1에 따라 이미 승인된 경우 제외). 전자 BCSI에 대한 프로비저닝된 전자 액세스		

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-004-7-R6-Part 6.1	각 책임 주체는 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 명시된 '해당 시스템'에 명시된 '해당 시스템'과 관련하여 BCSI에 대한 프로비저닝된 액세스를 승인, 확인 및 취소하기 위해 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 해당하는 각 요구 사항 부분을 모두 포함하는 하나 이상의 문서화된 액세스 관리 프로그램을 구현해야 합니다. 이 요구 사항의 맥락에서 BCSI에 대한 액세스 권한으로 간주되려면 개인은 BCSI를 획득하고 사용할 수 있는 능력을 모두 갖추고 있어야 합니다. 프로비저닝된 액세스는 개인에게 BCSI 액세스 수단(예: 물리적 키 또는 액세스 카드, 사용자 및 관련 권리/권한, 암호화 키)을 제공하기 위해 취해진 특정 조치의 결과로 간주됩니다. 섹션 6.1: CIP 예외적 상황을 제	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	외하고 책임 주체가 결정한 바에 따라 프로비저닝 전에 필요에 따라 권한을 부여합니다(섹션 4.1에 따라 이미 승인된 경우 제외). 전자 BCSI에 대한 프로비저닝된 전자 액세스		

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-004-7-R6-Part 6.1	각 책임 주체는 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 명시된 '해당 시스템'에 명시된 '해당 시스템'과 관련하여 BCSI에 대한 프로비저닝된 액세스를 승인, 확인 및 취소하기 위해 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 해당하는 각 요구 사항 부분을 모두 포함하는 하나 이상의 문서화된 액세스 관리 프로그램을 구현해야 합니다. 이 요구 사항의 맥락에서 BCSI에 대한 액세스 권한으로 간주되려면 개인은 BCSI를 획득하고 사용할 수 있는 능력을 모두 갖추고 있어야 합니다. 프로비저닝된 액세스는 개인에게 BCSI 액세스 수단(예: 물리적 키 또는 액세스 카드, 사용자 및 관련 권리/권한, 암호화 키)을 제공하기 위해 취해진 특정 조치의 결과로 간주됩니다. 섹션 6.1: CIP 예외적 상황을 제	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	외하고 책임 주체가 결정한 바에 따라 프로비저닝 전에 필요에 따라 권한을 부여합니다(섹션 4.1에 따라 이미 승인된 경우 제외). 전자 BCSI에 대한 프로비저닝된 전자 액세스		

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-004-7-R6-Part 6.1	각 책임 주체는 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 명시된 '해당 시스템'에 명시된 '해당 시스템'과 관련하여 BCSI에 대한 프로비저닝된 액세스를 승인, 확인 및 취소하기 위해 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 해당하는 각 요구 사항 부분을 모두 포함하는 하나 이상의 문서화된 액세스 관리 프로그램을 구현해야 합니다. 이 요구 사항의 맥락에서 BCSI에 대한 액세스 권한으로 간주되려면 개인은 BCSI를 획득하고 사용할 수 있는 능력을 모두 갖추고 있어야 합니다. 프로비저닝된 액세스는 개인에게 BCSI 액세스 수단(예: 물리적 키 또는 액세스 카드, 사용자 및 관련 권리/권한, 암호화 키)을 제공하기 위해 취해진 특정 조치의 결과로 간주됩니다. 섹션 6.1: CIP 예외적 상황을 제	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	외하고 책임 주체가 결정한 바에 따라 프로비저닝 전에 필요에 따라 권한을 부여합니다(섹션 4.1에 따라 이미 승인된 경우 제외). 전자 BCSI에 대한 프로비저닝된 전자 액세스		

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-004-7-R6-Part 6.1	각 책임 주체는 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 명시된 '해당 시스템'에 명시된 '해당 시스템'과 관련하여 BCSI에 대한 프로비저닝된 액세스를 승인, 확인 및 취소하기 위해 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 해당하는 각 요구 사항 부분을 모두 포함하는 하나 이상의 문서화된 액세스 관리 프로그램을 구현해야 합니다. 이 요구 사항의 맥락에서 BCSI에 대한 액세스 권한으로 간주되려면 개인은 BCSI를 획득하고 사용할 수 있는 능력을 모두 갖추고 있어야 합니다. 프로비저닝된 액세스는 개인에게 BCSI 액세스 수단(예: 물리적 키 또는 액세스 카드, 사용자 및 관련 권리/권한, 암호화 키)을 제공하기 위해 취해진 특정 조치의 결과로 간주됩니다. 섹션 6.1: CIP 예외적 상황을 제	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	외하고 책임 주체가 결정한 바에 따라 프로비저닝 전에 필요에 따라 권한을 부여합니다(섹션 4.1에 따라 이미 승인된 경우 제외). 전자 BCSI에 대한 프로비저닝된 전자 액세스		

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-004-7-R6-Part 6.1	각 책임 주체는 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 명시된 '해당 시스템'에 명시된 '해당 시스템'과 관련하여 BCSI에 대한 프로비저닝된 액세스를 승인, 확인 및 취소하기 위해 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 해당하는 각 요구 사항 부분을 모두 포함하는 하나 이상의 문서화된 액세스 관리 프로그램을 구현해야 합니다. 이 요구 사항의 맥락에서 BCSI에 대한 액세스 권한으로 간주되려면 개인은 BCSI를 획득하고 사용할 수 있는 능력을 모두 갖추고 있어야 합니다. 프로비저닝된 액세스는 개인에게 BCSI 액세스 수단(예: 물리적 키 또는 액세스 카드, 사용자 및 관련 권리/권한, 암호화 키)을 제공하기 위해 취해진 특정 조치의 결과로 간주됩니다. 섹션 6.1: CIP 예외적 상황을 제	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	외하고 책임 주체가 결정한 바에 따라 프로비저닝 전에 필요에 따라 권한을 부여합니다(섹션 4.1에 따라 이미 승인된 경우 제외). 전자 BCSI에 대한 프로비저닝된 전자 액세스		

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-004-7-R6-Part 6.1	각 책임 주체는 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 명시된 '해당 시스템'에 명시된 '해당 시스템'과 관련하여 BCSI에 대한 프로비저닝된 액세스를 승인, 확인 및 취소하기 위해 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 해당하는 각 요구 사항 부분을 모두 포함하는 하나 이상의 문서화된 액세스 관리 프로그램을 구현해야 합니다. 이 요구 사항의 맥락에서 BCSI에 대한 액세스 권한으로 간주되려면 개인은 BCSI를 획득하고 사용할 수 있는 능력을 모두 갖추고 있어야 합니다. 프로비저닝된 액세스는 개인에게 BCSI 액세스 수단(예: 물리적 키 또는 액세스 카드, 사용자 및 관련 권리/권한, 암호화 키)을 제공하기 위해 취해진 특정 조치의 결과로 간주됩니다. 섹션 6.1: CIP 예외적 상황을 제	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	외하고 책임 주체가 결정한 바에 따라 프로비저닝 전에 필요에 따라 권한을 부여합니다(섹션 4.1에 따라 이미 승인된 경우 제외). 전자 BCSI에 대한 프로비저닝된 전자 액세스		

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-004-7-R6-Part 6.1	각 책임 주체는 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 명시된 '해당 시스템'에 명시된 '해당 시스템'과 관련하여 BCSI에 대한 프로비저닝된 액세스를 승인, 확인 및 취소하기 위해 CIP-004-7 표 R6. BES 사이버 시스템 정보에 대한 액세스 관리에 해당하는 각 요구 사항 부분을 모두 포함하는 하나 이상의 문서화된 액세스 관리 프로그램을 구현해야 합니다. 이 요구 사항의 맥락에서 BCSI에 대한 액세스 권한으로 간주되려면 개인은 BCSI를 획득하고 사용할 수 있는 능력을 모두 갖추고 있어야 합니다. 프로비저닝된 액세스는 개인에게 BCSI 액세스 수단(예: 물리적 키 또는 액세스 카드, 사용자 및 관련 권리/권한, 암호화 키)을 제공하기 위해 취해진 특정 조치의 결과로 간주됩니다. 섹션 6.1: CIP 예외적 상황을 제	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	외하고 책임 주체가 결정한 바에 따라 프로비저닝 전에 필요에 따라 권한을 부여합니다(섹션 4.1에 따라 이미 승인된 경우 제외). 전자 BCSI에 대한 프로비저닝된 전자 액세스		
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository(ECR) 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	ecr-private-tag-immutability-enabled	Elastic Container Repository(ECR) 태그 변경 불가능 기능을 활성화하여 ECR 이미지의 이미지 태그를 덮어쓰지 않도록 합니다. 이전에는 태그를 덮어쓸 수 있었기 때문에 이미지를 고유하게 식별하기 위한 수동 방법이 필요했습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch와 다른 서비스 간에 보안 통신이 가능합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	s3-event-notifications-enabled	Amazon S3 이벤트 알림은 버킷 객체가 우발적이거나 의도적으로 수정된 경우 관련 담당자에게 알릴 수 있습니다. 알림의 예로는 새 객체 생성, 객체 제거, 객체 복원, 분실 및 복제된 객체 등이 있습니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	s3-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	rds-cluster-default-admin-check	기본 사용자 이름은 공개적으로 알려져 있으므로 기본 사용자 이름을 변경하면 Amazon Relational Database Service(RDS) 데이터베이스 클러스터의 공격 표면을 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	rds-instance-default-admin-check	기본 사용자 이름은 공개적으로 알려져 있으므로 기본 사용자 이름을 변경하면 Amazon Relational Database Service(RDS) 데이터베이스 클러스터의 공격 표면을 줄이는 데 도움이 됩니다.
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	redshift-default-admin-check	기본 사용자 이름은 공개적으로 알려져 있으므로 기본 사용자 이름을 변경하면 Amazon Redshift 클러스터의 공격 표면을 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CIP-011-3-R1-Part 1.2	각 책임 주체는 CIP-011-3 표 R1. 정보 보호의 해당 요구 사항 각 부분을 총체적으로 포함하는 문서화된 정보 보호 프로그램을 하나 이상 구현해야 합니다. 섹션 1.2: BCSI를 보호하고 안전하게 처리하여 기밀 침해 위험을 완화하는 방법	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

템플릿

템플릿은 GitHub: NERC CIP BCSI 운영 모범 사례에서 확인할 수 있습니다.

NCSC 클라우드 보안 원칙 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 영국 국가 사이버 보안 센터(NCSC) 클라우드 보안 원칙과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 UK NCSC 클라우드 보안 원칙 제어와 관련이 있습니다. 영국 NCSC 클라우드 보안 원칙 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 샘플 적합성 팩 템플릿에는 영국 NCSC 클라우드 보안 원칙(National Cyber Security Centre | 클라우드 보안 지침) 내 제어에 대한 매핑이 포함되어 있으며, 이러한 공공 부문 정보는 Open Government

Licence v3.0에 따라 라이선스가 부여됩니다. Open Government Licence는 Open Government Licence for public sector information에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1. 전송 중 데이터 보호	사용자 데이터를 전송하는 네트워크는 변조 및 도청으로부터 적절하게 보호되어야 합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
1. 전송 중 데이터 보호	사용자 데이터를 전송하는 네트워크는 변조 및 도청으로부터 적절하게 보호되어야 합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
1. 전송 중 데이터 보호	사용자 데이터를 전송하는 네트워크는 변조 및 도청으로부터 적절	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호

제어 ID	제어 설명	AWS 구성 규칙	지침
	하게 보호되어야 합니다.		화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1. 전송 중 데이터 보호	사용자 데이터를 전송하는 네트워크는 변조 및 도청으로부터 적절하게 보호되어야 합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증하는지 확인합니다.
1. 전송 중 데이터 보호	사용자 데이터를 전송하는 네트워크는 변조 및 도청으로부터 적절하게 보호되어야 합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1. 전송 중 데이터 보호	사용자 데이터를 전송하는 네트워크는 변조 및 도청으로부터 적절하게 보호되어야 합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
1. 전송 중 데이터 보호	사용자 데이터를 전송하는 네트워크는 변조 및 도청으로부터 적절하게 보호되어야 합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1. 전송 중 데이터 보호	사용자 데이터를 전송하는 네트워크는 변조 및 도청으로부터 적절하게 보호되어야 합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1. 전송 중 데이터 보호	사용자 데이터를 전송하는 네트워크는 변조 및 도청으로부터 적절하게 보호되어야 합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1. 전송 중 데이터 보호	사용자 데이터를 전송하는 네트워크는 변조 및 도청으로부터 적절하게 보호되어야 합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1. 전송 중 데이터 보호	사용자 데이터를 전송하는 네트워크는 변조 및 도청으로부터 적절하게 보호되어야 합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하는 데 도움이 되도록 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2. 자산 보호 및 복원력	데이터(및 데이터를 저장하거나 처리하는 자산)는 적절하게 보호되어야 합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
5. 운영 보안	서비스는 공격을 방해, 탐지 또는 방지하는 방식으로 운영 및 관리되어야 합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7. 안전한 개발	클라우드 서비스는 보안에 대한 위협을 최소화하고 완화하는 방식으로 설계, 개발 및 배포되어야 합니다.	codebuild-project-environment-privileged-check	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있지 않은지 확인합니다. Docker API와 컨테이너의 기본 하드웨어에 대해 의도하지 않은 액세스를 방지하려면 이 설정을 비활성화해야 합니다.
7. 안전한 개발	클라우드 서비스는 보안에 대한 위협을 최소화하고 완화하는 방식으로 설계, 개발 및 배포되어야 합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7. 안전한 개발	클라우드 서비스는 보안에 대한 위협을 최소화하고 완화하는 방식으로 설계, 개발 및 배포되어야 합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
9. 보안 사용자 관리	제공업체는 서비스 사용을 안전하게 관리할 수 있는 도구를 제공해야 합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10. ID 및 인증	서비스 인터페이스에 대한 액세스는 인증되고 승인된 개인으로 제한되어야 합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
10. ID 및 인증	서비스 인터페이스에 대한 액세스는 인증되고 승인된 개인으로 제한되어야 합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10. ID 및 인증	서비스 인터페이스에 대한 액세스는 인증되고 승인된 개인으로 제한되어야 합니다.	rds-instance-iam-authentication-enabled	시스템 및 자산에 대한 액세스를 제어하기 위해 Amazon Relational Database Service(Amazon RDS) 인스턴스에서 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. 이렇게 하면 데이터베이스를 오가는 네트워크 트래픽이 SSL(Secure Sockets Layer)을 통해 암호화됩니다. 인증은 외부에서 관리되므로 사용자 보안 인증 정보를 데이터베이스에 저장할 필요가 없습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10. ID 및 인증	서비스 인터페이스에 대한 액세스는 인증되고 승인된 개인으로 제한되어야 합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10. ID 및 인증	서비스 인터페이스에 대한 액세스는 인증되고 승인된 개인으로 제한되어야 합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10. ID 및 인증	서비스 인터페이스에 대한 액세스는 인증되고 승인된 개인으로 제한되어야 합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
10. ID 및 인증	서비스 인터페이스에 대한 액세스는 인증되고 승인된 개인으로 제한되어야 합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
10. ID 및 인증	서비스 인터페이스에 대한 액세스는 인증되고 승인된 개인으로 제한되어야 합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10. ID 및 인증	서비스 인터페이스에 대한 액세스는 인증되고 승인된 개인으로 제한되어야 합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
10. ID 및 인증	서비스 인터페이스에 대한 액세스는 인증되고 승인된 개인으로 제한되어야 합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 방어해야 합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	ecs-container-insights-enabled	모니터링은 Amazon Elastic Container Service(ECS) 및 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. 또한 Container Insights는 컨테이너 재시작 오류 같은 진단 정보를 제공하여 문제를 격리하고 신속하게 해결할 수 있도록 도와줍니다.
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11. 외부 인터페이스 보호	서비스에 대한 외부 또는 신뢰도가 낮은 모든 인터페이스를 식별하고 보호해야 합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12. 보안 서비스 관리	클라우드 제공업체는 관리 시스템의 높은 가치를 인식해야 합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
13. 사용자를 위한 감사 정보	제공업체는 서비스에 대한 액세스를 모니터링하는 데 필요한 로그와 서비스 내에 보관된 데이터를 제공해야 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13. 사용자를 위한 감사 정보	제공업체는 서비스에 대한 액세스를 모니터링하는 데 필요한 로그와 서비스 내에 보관된 데이터를 제공해야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
13. 사용자를 위한 감사 정보	제공업체는 서비스에 대한 액세스를 모니터링하는 데 필요한 로그와 서비스 내에 보관된 데이터를 제공해야 합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
13. 사용자를 위한 감사 정보	제공업체는 서비스에 대한 액세스를 모니터링하는 데 필요한 로그와 서비스 내에 보관된 데이터를 제공해야 합니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail의 사용이 포함됩니다.

템플릿

템플릿은 GitHub: NCSC 클라우드 보안 원칙 운영 모범 사례에서 확인할 수 있습니다.

NCSC 사이버 평가 프레임워크 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 영국 국가 사이버 보안 센터(NCSC) 사이버 평가 프레임워크(CAF) 제어와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 UK NCSC CAF 제어와 관련이 있습니다. 영국 NCSC CAF 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 샘플 적합성 팩 템플릿에는 영국 NCSC CAF (National Cyber Security Centre | NCSC CAF 지침) 내의 제어에 대한 매핑이 포함되어 있으며, 해당 공공 부문 정보는 Open Government Licence v3.0에 따라 사용이 허가되었습니다. Open Government Licence는 Open Government Licence for public sector information에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.a.#자산 관리	필수 기능 운영에 필요한 네트워크 및 정보 시스템을 제공, 유지 또는 지원하는 데 필요한 모든 것을 결정하고 이해합니다. 여기에는 데이터, 인력, 시스템은 물론 모든 지원 인프라(예: 전력 또는 냉각)도 포함됩니다.	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
A3.a.#자산 관리	필수 기능 운영에 필요한 네트워크 및 정보 시스템을 제공, 유지 또는 지원하는 데 필요한 모든 것을 결정하고 이해합니다. 여기에는 데이터, 인력, 시스템은 물론 모든 지원 인프라(예: 전력 또는 냉각)도 포함됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
A3.a.#자산 관리	필수 기능 운영에 필요한 네트워크 및 정보 시스템을 제공, 유지	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인

제어 ID	제어 설명	AWS 구성 규칙	지침
	또는 지원하는 데 필요한 모든 것을 결정하고 이해합니다. 여기에는 데이터, 인력, 시스템은 물론 모든 지원 인프라(예: 전력 또는 냉각)도 포함됩니다.		스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
A3.a.#자산 관리	필수 기능 운영에 필요한 네트워크 및 정보 시스템을 제공, 유지 또는 지원하는 데 필요한 모든 것을 결정하고 이해합니다. 여기에는 데이터, 인력, 시스템은 물론 모든 지원 인프라(예: 전력 또는 냉각)도 포함됩니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.a.#자산 관리	필수 기능 운영에 필요한 네트워크 및 정보 시스템을 제공, 유지 또는 지원하는 데 필요한 모든 것을 결정하고 이해합니다. 여기에는 데이터, 인력, 시스템은 물론 모든 지원 인프라(예: 전력 또는 냉각)도 포함됩니다.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.a#Identity Verification, Authentication and Authorisation	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
B2.a Identity Verification,Authentication and Authorisation	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.a. ID 확인, 인증 및 승인	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 액세스를 엄격하게 확인, 인증 및 승인합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.b. 디바이스 관리	필수 기능을 지원하는 네트워크, 정보 시스템 및 데이터에 액세스하는 데 사용되는 장치를 충분히 알고 있고 신뢰할 수 있습니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.b. 디바이스 관리	필수 기능을 지원하는 네트워크, 정보 시스템 및 데이터에 액세스하는 데 사용되는 장치를 충분히 알고 있고 신뢰할 수 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	codebuild-project-environment-privileged-check	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있지 않은지 확인합니다. Docker API와 컨테이너의 기본 하드웨어에 대해 의도하지 않은 액세스를 방지하려면 이 설정을 비활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	secretsmanager-secret-unused	AWS Secrets Manager에 미사용 자격 증명이 있는 경우 자격 증명을 비활성화 및/또는 제거해야 합니다. 최소 권한 원칙을 위반할 수 있습니다. 이 규칙을 사용하면 값을 unusedForDays(Config 기본값: 90)로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.c. 권한 있는 사용자 관리	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 권한 있는 사용자 액세스를 면밀히 관리합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B2.d. ID 및 액세스 관리(iDAM)	필수 기능을 지원하는 네트워크 및 정보 시스템에 대한 ID 및 액세스 제어를 잘 관리하고 유지할 수 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.a. 데이터 이해	필수 기능 운영에 중요한 데이터의 저장 위치, 이동 경로 및 사용 불가 또는 무단 액세스, 수정 또는 삭제가 필수 기능에 미치는 악영향을 잘 알고 있습니다. 이는 필수 기능 운영에 중요한 데이터를 저장하거나 액세스하는 제3자에게도 적용됩니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.b. 전송 중 데이터	필수 기능 운영에 중요한 데이터 전송을 보호해야 합니다. 여기에는 제3자로의 데이터 전송도 포함됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호하고 있습니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
B3.c. 저장된 데이터	필수 기능 작동에 중요한 저장된 데이터를 보호해야 합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.a. 보안 설계	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템에 보안을 설계합니다. 공격 표면을 최소화하고 단일 취약점의 악용에 의해 필수 기능의 작동이 영향을 받지 않도록 해야 합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.b. 보안 구성	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템을 안전하게 구성합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
B4.b. 보안 구성	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템을 안전하게 구성합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.b. 보안 구성	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템을 안전하게 구성합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.b. 보안 구성	필수 기능의 운영을 지원하는 네트워크 및 정보 시스템을 안전하게 구성합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.c. 보안 관리	보안을 활성화하고 유지하기 위한 필수 기능의 운영을 지원하는 조직의 네트워크 및 정보 시스템을 관리합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
B4.c. 보안 관리	보안을 활성화하고 유지하기 위한 필수 기능의 운영을 지원하는 조직의 네트워크 및 정보 시스템을 관리합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.c. 보안 관리	보안을 활성화하고 유지하기 위한 필수 기능의 운영을 지원하는 조직의 네트워크 및 정보 시스템을 관리합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.d. 취약성 관리	네트워크 및 정보 시스템의 알려진 취약성을 관리하여 필수 기능에 부정적인 영향을 미치지 않도록 합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
B4.d. 취약성 관리	네트워크 및 정보 시스템의 알려진 취약성을 관리하여 필수 기능에 부정적인 영향을 미치지 않도록 합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.d. 취약성 관리	네트워크 및 정보 시스템의 알려진 취약성을 관리하여 필수 기능에 부정적인 영향을 미치지 않도록 합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.d. 취약성 관리	네트워크 및 정보 시스템의 알려진 취약성을 관리하여 필수 기능에 부정적인 영향을 미치지 않도록 합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.d. 취약성 관리	네트워크 및 정보 시스템의 알려진 취약성을 관리하여 필수 기능에 부정적인 영향을 미치지 않도록 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B4.d. 취약성 관리	네트워크 및 정보 시스템의 알려진 취약성을 관리하여 필수 기능에 부정적인 영향을 미치지 않도록 합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B5.b. 복원력을 위한 설계	사이버 보안 인시던트에 대응할 수 있도록 필수 기능을 지원하는 네트워크 및 정보 시스템을 설계합니다. 시스템을 적절히 분리하고 리소스 제한을 완화합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B5.b. 복원력을 위한 설계	사이버 보안 인시던트에 대응할 수 있도록 필수 기능을 지원하는 네트워크 및 정보 시스템을 설계합니다. 시스템을 적절히 분리하고 리소스 제한을 완화합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B5.b. 복원력을 위한 설계	사이버 보안 인시던트에 대응할 수 있도록 필수 기능을 지원하는 네트워크 및 정보 시스템을 설계합니다. 시스템을 적절히 분리하고 리소스 제한을 완화합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
B5.c. 백업	필수 기능의 작동을 복구하는 데 필요한 데이터 및 정보의 접근 가능하고 안전한 최신 백업을 보유해야 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B5.c. 백업	필수 기능의 작동을 복구하는 데 필요한 데이터 및 정보의 접근 가능하고 안전한 최신 백업을 보유해야 합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
B5.c. 백업	필수 기능의 작동을 복구하는 데 필요한 데이터 및 정보의 접근 가능하고 안전한 최신 백업을 보유해야 합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B5.c. 백업	필수 기능의 작동을 복구하는 데 필요한 데이터 및 정보의 접근 가능하고 안전한 최신 백업을 보유해야 합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
B5.c. 백업	필수 기능의 작동을 복구하는 데 필요한 데이터 및 정보의 접근 가능하고 안전한 최신 백업을 보유해야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B5.c. 백업	필수 기능의 작동을 복구하는 데 필요한 데이터 및 정보의 접근 가능하고 안전한 최신 백업을 보유해야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
B5.c. 백업	필수 기능의 작동을 복구하는 데 필요한 데이터 및 정보의 접근 가능하고 안전한 최신 백업을 보유해야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B5.c. 백업	필수 기능의 작동을 복구하는 데 필요한 데이터 및 정보의 접근 가능하고 안전한 최신 백업을 보유해야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
B5.c. 백업	필수 기능의 작동을 복구하는 데 필요한 데이터 및 정보의 접근 가능하고 안전한 최신 백업을 보유해야 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
B5.c. 백업	필수 기능의 작동을 복구하는 데 필요한 데이터 및 정보의 접근 가능하고 안전한 최신 백업을 보유해야 합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
C1.a. 모니터링 범위	모니터링에 포함하는 데이터 소스를 통해 필수 기능 운영에 영향을 미칠 수 있는 보안 이벤트를 적시에 식별할 수 있어야 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.a. 모니터링 범위	모니터링에 포함하는 데이터 소스를 통해 필수 기능 운영에 영향을 미칠 수 있는 보안 이벤트를 적시에 식별할 수 있어야 합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.a. 모니터링 범위	모니터링에 포함하는 데이터 소스를 통해 필수 기능 운영에 영향을 미칠 수 있는 보안 이벤트를 적시에 식별할 수 있어야 합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.a. 모니터링 범위	모니터링에 포함하는 데이터 소스를 통해 필수 기능 운영에 영향을 미칠 수 있는 보안 이벤트를 적시에 식별할 수 있어야 합니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
C1.a. 모니터링 범위	모니터링에 포함하는 데이터 소스를 통해 필수 기능 운영에 영향을 미칠 수 있는 보안 이벤트를 적시에 식별할 수 있어야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.a. 모니터링 범위	모니터링에 포함하는 데이터 소스를 통해 필수 기능 운영에 영향을 미칠 수 있는 보안 이벤트를 적시에 식별할 수 있어야 합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
C1.a. 모니터링 범위	모니터링에 포함하는 데이터 소스를 통해 필수 기능 운영에 영향을 미칠 수 있는 보안 이벤트를 적시에 식별할 수 있어야 합니다.	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.a. 모니터링 범위	모니터링에 포함하는 데이터 소스를 통해 필수 기능 운영에 영향을 미칠 수 있는 보안 이벤트를 적시에 식별할 수 있어야 합니다.	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.a. 모니터링 범위	모니터링에 포함하는 데이터 소스를 통해 필수 기능 운영에 영향을 미칠 수 있는 보안 이벤트를 적시에 식별할 수 있어야 합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.a. 모니터링 범위	모니터링에 포함하는 데이터 소스를 통해 필수 기능 운영에 영향을 미칠 수 있는 보안 이벤트를 적시에 식별할 수 있어야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
C1.a. 모니터링 범위	모니터링에 포함하는 데이터 소스를 통해 필수 기능 운영에 영향을 미칠 수 있는 보안 이벤트를 적시에 식별할 수 있어야 합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.b. 보안 로그	로깅 데이터를 안전하게 보관하고 업무상 필요한 계정에만 읽기 권한을 부여합니다. 어떤 직원도 합의된 보존 기간 내에 로깅 데이터를 수정하거나 삭제할 필요가 없으며, 그 이후에는 삭제해야 합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.b. 보안 로그	로깅 데이터를 안전하게 보관하고 업무상 필요한 계정에만 읽기 권한을 부여합니다. 어떤 직원도 합의된 보존 기간 내에 로깅 데이터를 수정하거나 삭제할 필요가 없으며, 그 이후에는 삭제해야 합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
C1.b. 보안 로그	로깅 데이터를 안전하게 보관하고 업무상 필요한 계정에만 읽기 권한을 부여합니다. 어떤 직원도 합의된 보존 기간 내에 로깅 데이터를 수정하거나 삭제할 필요가 없으며, 그 이후에는 삭제해야 합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.b. 보안 로그	로깅 데이터를 안전하게 보관하고 업무상 필요한 계정에만 읽기 권한을 부여합니다. 어떤 직원도 합의된 보존 기간 내에 로깅 데이터를 수정하거나 삭제할 필요가 없으며, 그 이후에는 삭제해야 합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
C1.b. 보안 로그	로깅 데이터를 안전하게 보관하고 업무상 필요한 계정에만 읽기 권한을 부여합니다. 어떤 직원도 합의된 보존 기간 내에 로깅 데이터를 수정하거나 삭제할 필요가 없으며, 그 이후에는 삭제해야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.b. 보안 로그	로깅 데이터를 안전하게 보관하고 업무상 필요한 계정에만 읽기 권한을 부여합니다. 어떤 직원도 합의된 보존 기간 내에 로깅 데이터를 수정하거나 삭제할 필요가 없으며, 그 이후에는 삭제해야 합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
C1.b. 보안 로그	로깅 데이터를 안전하게 보관하고 업무상 필요한 계정에만 읽기 권한을 부여합니다. 어떤 직원도 합의된 보존 기간 내에 로깅 데이터를 수정하거나 삭제할 필요가 없으며, 그 이후에는 삭제해야 합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.b. 보안 로그	로깅 데이터를 안전하게 보관하고 업무상 필요한 계정에만 읽기 권한을 부여합니다. 어떤 직원도 합의된 보존 기간 내에 로깅 데이터를 수정하거나 삭제할 필요가 없으며, 그 이후에는 삭제해야 합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
C1.b. 보안 로그	로깅 데이터를 안전하게 보관하고 업무상 필요한 계정에만 읽기 권한을 부여합니다. 어떤 직원도 합의된 보존 기간 내에 로깅 데이터를 수정하거나 삭제할 필요가 없으며, 그 이후에는 삭제해야 합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.b. 보안 로그	로깅 데이터를 안전하게 보관하고 업무상 필요한 계정에만 읽기 권한을 부여합니다. 어떤 직원도 합의된 보존 기간 내에 로깅 데이터를 수정하거나 삭제할 필요가 없으며, 그 이후에는 삭제해야 합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.b. 보안 로그	로깅 데이터를 안전하게 보관하고 업무상 필요한 계정에만 읽기 권한을 부여합니다. 어떤 직원도 합의된 보존 기간 내에 로깅 데이터를 수정하거나 삭제할 필요가 없으며, 그 이후에는 삭제해야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 경고를 트리거합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	s3-event-notifications-enabled	Amazon S3 이벤트 알림은 버킷 객체가 우발적이거나 의도적으로 수정된 경우 관련 담당자에게 알릴 수 있습니다. 알림의 예로는 새 객체 생성, 객체 제거, 객체 복원, 분실 및 복제된 객체 등이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
C1.c. 알림 생성	모니터링 데이터에 포함된 잠재적 보안 인시던트의 증거를 확실하게 식별하여 알림을 트리거합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.d. 보안 사고 식별	위협 및 시스템에 대한 지식을 바탕으로 알림을 컨텍스트화하여 특정 형태의 대응이 필요한 보안 인시던트를 식별합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.d. 보안 사고 식별	위협 및 시스템에 대한 지식을 바탕으로 알림을 컨텍스트화하여 특정 형태의 대응이 필요한 보안 인시던트를 식별합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
C1.e. 모니터링 도구 및 기술	아웃소싱된 것을 포함하여 직원의 기술, 도구 및 역할을 모니터링할 때는 거버넌스 및 보고 요구 사항, 예상되는 위협, 이들이 사용해야 하는 네트워크 또는 시스템 데이터의 복잡성을 반영해야 합니다. 모니터링 직원은 보호해야 할 필수 기능을 잘 알고 있습니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.e. 모니터링 도구 및 기술	아웃소싱된 것을 포함하여 직원의 기술, 도구 및 역할을 모니터링할 때는 거버넌스 및 보고 요구 사항, 예상되는 위협, 이들이 사용해야 하는 네트워크 또는 시스템 데이터의 복잡성을 반영해야 합니다. 모니터링 직원은 보호해야 할 필수 기능을 잘 알고 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C1.e. 모니터링 도구 및 기술	아웃소싱된 것을 포함하여 직원의 기술, 도구 및 역할을 모니터링할 때는 거버넌스 및 보고 요구 사항, 예상되는 위협, 이들이 사용해야 하는 네트워크 또는 시스템 데이터의 복잡성을 반영해야 합니다. 모니터링 직원은 보호해야 할 필수 기능을 잘 알고 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C2.a. 공격 탐지를 위한 시스템 이상	식별하기 어려운 악의적인 활동을 탐지할 수 있는 실용적인 방법을 제공하는 시스템 동작의 이상 사례를 정의합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
C2.a. 공격 탐지를 위한 시스템 이상	식별하기 어려운 악의적인 활동을 탐지할 수 있는 실용적인 방법을 제공하는 시스템 동작의 이상 사례를 정의합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
D1.c. 테스트 및 연습	조직은 조직(및 다른 조직)에 영향을 미친 과거 인시던트와 위협 인텔리전스 및 위험 평가를 기반으로 하는 시나리오를 사용하여 대응 계획을 테스트하는 연습을 수행합니다.	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되는지 확인하세요. 대응 계획을 업데이트하고 공식적으로 문서화하면 대응 담당자가 역할, 책임 및 사고 발생 시 따라야 할 프로세스를 이해하는 데 도움이 될 수 있습니다.
D1.c. 테스트 및 연습	조직은 조직(및 다른 조직)에 영향을 미친 과거 인시던트와 위협 인텔리전스 및 위험 평가를 기반으로 하는 시나리오를 사용하여 대응 계획을 테스트하는 연습을 수행합니다.	response-plan-tested(프로세스 확인)	사고 대응 및 복구 계획이 테스트되었는지 확인합니다. 이는 인시던트 발생 중에 해당 계획이 효과적인지 그리고 격차나 업데이트를 해결해야 하는지를 이해하는 데 도움이 될 수 있습니다.

템플릿

템플릿은 GitHub: NCSC 사이버 평가 프레임워크 운영 모범 사례에서 확인할 수 있습니다.

네트워킹 및 콘텐츠 전송 서비스 운영 모범 사례

이 적합성 팩에는 네트워킹 및 콘텐츠 전송 서비스에 기반한 AWS Config 규칙이 포함되어 있습니다. 자세한 내용은 네트워킹 및 콘텐츠 전송을 AWS 참조하세요. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 네트워킹 및 콘텐츠 전송 서비스 운영 모범 사례에서 확인할 수 있습니다.

NIST 800-53 rev 4 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 NIST 800-53과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 NIST 800-53 제어와 관련이 있습니다. NIST 800-53 제어는 여러 구성 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

이 적합성 팩은 Payment Card Industry Qualified Security Assessors(QSAs), HITRUST Certified Common Security Framework Practitioners(CCSFPs) 및 다양한 산업 프레임워크에 대한 지침과 평가를 제공하도록 인증된 규정 준수 전문가로 구성된 팀인 AWS Security Assurance Services LLC(AWS SA AWS S)에서 검증되었습니다.SAS 전문가는 고객이 NIST 800-53의 하위 집합에 맞게이 적합성 팩을 설계했습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으

제어 ID	제어 설명	AWS Config 규칙	지침
			로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 CIS(인터넷 보안 센터) AWS 파운데이션 벤치마크의 암호 강도에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS Config 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(1)	조직은 자동화된 메커니즘을 사용하여 정보 시스템 계정 관리를 지원합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(3)	정보 시스템은 [할당: 조직에서 정의한 기간]이 지나면 비활성 계정을 자동으로 비활성화합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	cloudtrail-enabled	AWS CloudTrail 는 Management Console 작업 및 API 호출을 기록 AWS 하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	multi-region-cloudtrail-enabled	AWS CloudTrail 는 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든에서 S3 버킷 AWS 리전으로 로그 파일을 전송합니다. 또한 AWS 에서 새 리전을 시작하면 CloudTrail은 새 리전에 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(4)	정보 시스템은 계정 생성, 수정, 활성화, 비활성화 및 제거 작업을 자동으로 감사하고 [할당: 조직에서 정의한 직원 또는 역할]을 알립니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(12)(a)	조직: a. 정보 시스템 계정의 [할당: 조직에서 정의한 비정형 용도] 활동을 모니터링합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(12)(a)	조직: a. 정보 시스템 계정의 [할당: 조직에서 정의한 비정형 용도] 활동을 모니터링합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 CIS(인터넷 보안 센터) AWS 파운데이션 벤치마크의 암호 강도에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS Config 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2(f)	조직: f. [할당: 조직에서 정의한 절차 또는 조건]에 따라 정보 시스템 계정을 생성, 활성화, 수정, 비활성화 및 제거합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	cloudtrail-enabled	AWS CloudTrail 는 Management Console 작업 및 API 호출을 기록 AWS 하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(g)	조직: g. 정보 시스템 계정 사용을 모니터링합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 CIS(인터넷 보안 센터) AWS 파운데이션 벤치마크의 암호 강도에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS Config 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-2(j)	조직: j. 계정이 계정 관리 요구 사항을 준수하는지 [할당: 조직에서 정의한 빈도]로 검토합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	s3-account-level-public-access-blocks	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-3	정보 시스템은 해당 액세스 제어 정책에 따라 정보 및 시스템 리소스에 대한 논리적 액세스에 대해 승인된 권한을 적용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	s3-account-level-public-access-blocks	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-4	정보 시스템은 [할당: 조직이 정의한 정보 흐름 제어 정책]에 따라 시스템 내 및 상호 연결된 시스템 간의 정보 흐름을 제어할 수 있는 승인된 권한을 적용합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-5c	조직: c. 업무 분리를 지원하는 정보 시스템 액세스 권한을 정의합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-account-level-public-access-blocks	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
AC-6	조직은 최소 권한 원칙을 이용하여 조직의 임무 및 업무 기능에 따라 할당된 작업을 수행하는 데 필요한 사용자(또는 사용자를 대신하는 프로세스)에 대한 승인된 액세스만 허용합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-6(10)	정보 시스템은 권한이 없는 사용자가 구현된 보안 보호 장치 및 대응 조치를 비활성화, 우회 또는 변경하는 것을 포함하는 권한 있는 기능을 실행하는 것을 방지합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-17(1)	정보 시스템은 원격 액세스 방법을 모니터링하고 제어합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC-17(2)	정보 시스템은 암호화 메커니즘을 구현하여 원격 액세스 세션의 기밀성과 무결성을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-17(3)	정보 시스템은 [할당: 조직에서 정의한 번호] 개수의 관리 네트워크 액세스 제어 지점을 통해 모든 원격 액세스를 라우팅합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	s3-account-level-public-access-blocks	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AC-21(b)	조직: b. [할당: 조직에서 정의한 자동화 메커니즘 또는 수동 프로세스]를 사용하여 사용자가 정보 공유 및 협업 결정을 내리는 데 도움을 줍니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
AU-2(a)(d)	조직 a: 정보 시스템이 [할당: 조직 정의 감사 가능 이벤트]를 감사할 수 있는지 결정합니다. 정보 시스템 내에서 다음과 같은 이벤트를 감사할 것인지 결정합니다. [할당: 조직에서 정의한 감사 이벤트 (AU-2 a에 정의된 감사 대상 이벤트의 하위 집합) 및 식별된 각 이벤트에 대한 감사 빈도 (또는 필요한 상황)]	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-2(a)(d)	조직 a: 정보 시스템이 [할당: 조직 정의 감사 가능 이벤트]를 감사할 수 있는지 결정합니다. 조직 d: 정보 시스템 내에서 다음과 같은 이벤트를 감사할 것인지 결정합니다. [할당: 조직에서 정의한 감사 이벤트(AU-2 a에 정의된 감사 대상 이벤트의 하위 집합) 및 식별된 각 이벤트에 대한 감사 빈도(또는 필요한 상황)]	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-2(a)(d)	조직 a: 정보 시스템이 [할당: 조직 정의 감사 가능 이벤트]를 감사할 수 있는지 결정합니다. 조직 d: 정보 시스템 내에서 다음과 같은 이벤트를 감사할 것인지 결정합니다. [할당: 조직에서 정의한 감사 이벤트(AU-2 a에 정의된 감사 대상 이벤트의 하위 집합) 및 식별된 각 이벤트에 대한 감사 빈도(또는 필요한 상황)]	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-2(a)(d)	조직 a: 정보 시스템이 [할당: 조직 정의 감사 가능 이벤트]를 감사할 수 있는지 결정합니다. 조직 d: 정보 시스템 내에서 다음과 같은 이벤트를 감사할 것인지 결정합니다. [할당: 조직에서 정의한 감사 이벤트(AU-2 a에 정의된 감사 대상 이벤트의 하위 집합) 및 식별된 각 이벤트에 대한 감사 빈도(또는 필요한 상황)]	cloudtrail-enabled	AWS CloudTrail 는 Management Console 작업 및 API 호출을 기록 AWS 하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-2(a)(d)	조직 a: 정보 시스템이 [할당: 조직 정의 감사 가능 이벤트]를 감사할 수 있는지 결정합니다. 조직 d: 정보 시스템 내에서 다음과 같은 이벤트를 감사할 것인지 결정합니다. [할당: 조직에서 정의한 감사 이벤트(AU-2 a에 정의된 감사 대상 이벤트의 하위 집합) 및 식별된 각 이벤트에 대한 감사 빈도(또는 필요한 상황)]	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-2(a)(d)	조직 a: 정보 시스템이 [할당: 조직 정의 감사 가능 이벤트]를 감사할 수 있는지 결정합니다. 조직 d: 정보 시스템 내에서 다음과 같은 이벤트를 감사할 것인지 결정합니다. [할당: 조직에서 정의한 감사 이벤트(AU-2 a에 정의된 감사 대상 이벤트의 하위 집합) 및 식별된 각 이벤트에 대한 감사 빈도(또는 필요한 상황)]	multi-region-cloudtrail-enabled	AWS CloudTrail 는 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든에서 S3 버킷 AWS 리전으로 로그 파일을 전송합니다. 또한 AWS 에서 새 리전을 시작하면 CloudTrail은 새 리전에 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-2(a)(d)	조직 a: 정보 시스템이 [할당: 조직 정의 감사 가능 이벤트]를 감사할 수 있는지 결정합니다. 조직 d: 정보 시스템 내에서 다음과 같은 이벤트를 감사할 것인지 결정합니다. [할당: 조직에서 정의한 감사 이벤트(AU-2 a에 정의된 감사 대상 이벤트의 하위 집합) 및 식별된 각 이벤트에 대한 감사 빈도(또는 필요한 상황)]	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-2(a)(d)	조직 a: 정보 시스템이 [할당: 조직 정의 감사 가능 이벤트]를 감사할 수 있는지 결정합니다. 조직 d: 정보 시스템 내에서 다음과 같은 이벤트를 감사할 것인지 결정합니다. [할당: 조직에서 정의한 감사 이벤트(AU-2 a에 정의된 감사 대상 이벤트의 하위 집합) 및 식별된 각 이벤트에 대한 감사 빈도(또는 필요한 상황)]	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
AU-2(a)(d)	조직 a: 정보 시스템이 [할당: 조직 정의 감사 가능 이벤트]를 감사할 수 있는지 결정합니다. 조직 d: 정보 시스템 내에서 다음과 같은 이벤트를 감사할 것인지 결정합니다. [할당: 조직에서 정의한 감사 이벤트(AU-2 a에 정의된 감사 대상 이벤트의 하위 집합) 및 식별된 각 이벤트에 대한 감사 빈도(또는 필요한 상황)]	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-2(a)(d)	조직 a: 정보 시스템이 [할당: 조직 정의 감사 가능 이벤트]를 감사할 수 있는지 결정합니다. 조직 d: 정보 시스템 내에서 다음과 같은 이벤트를 감사할 것인지 결정합니다. [할당: 조직에서 정의한 감사 이벤트(AU-2 a에 정의된 감사 대상 이벤트의 하위 집합) 및 식별된 각 이벤트에 대한 감사 빈도(또는 필요한 상황)]	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-2(a)(d)	조직 a: 정보 시스템이 [할당: 조직 정의 감사 가능 이벤트]를 감사할 수 있는지 결정합니다. 조직 d: 정보 시스템 내에서 다음과 같은 이벤트를 감사할 것인지 결정합니다. [할당: 조직에서 정의한 감사 이벤트(AU-2 a에 정의된 감사 대상 이벤트의 하위 집합) 및 식별된 각 이벤트에 대한 감사 빈도(또는 필요한 상황)]	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	cloudtrail-enabled	AWS CloudTrail 는 Management Console 작업 및 API 호출을 기록 AWS 하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail 는 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든에서 S3 버킷 AWS 리전으로 로그 파일을 전송합니다. 또한 AWS 에서 새 리전을 시작하면 CloudTrail은 새 리전에 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-3	정보 시스템은 어떤 유형의 이벤트가 발생했는지, 언제 발생했는지, 어디서 발생했는지, 이벤트의 출처, 이벤트 결과, 이벤트와 관련된 개인 또는 주체의 ID를 확인하는 정보가 포함된 감사 기록을 생성합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-6(1)(3)	(1) 조직은 자동화된 메커니즘을 사용하여 감사 검토, 분석 및 보고 프로세스를 통합하여 의심스러운 활동에 대한 조사 및 대응을 위한 조직 프로세스를 지원합니다. (3) 조직은 여러 리포지토리의 감사 기록을 분석하고 상호 연관시켜 조직 전반의 상황을 파악합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-7(1)	정보 시스템은 [할당: 감사 기록 내 조직이 정의한 감사 필드]를 기반으로 관심 이벤트에 대한 감사 기록을 처리할 수 있는 기능을 제공합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
AU-7(1)	정보 시스템은 [할당: 감사 기록 내 조직이 정의한 감사 필드]를 기반으로 관심 이벤트에 대한 감사 기록을 처리할 수 있는 기능을 제공합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-9	정보 시스템은 감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
AU-9	정보 시스템은 감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
AU-9(2)	정보 시스템은 감사 기록을 [할당: 조직이 정의한 빈도]로 감사 대상 시스템 또는 구성 요소와 물리적으로 다른 시스템 또는 시스템 구성 요소에 백업합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-11	조직은 보안 사고에 대한 사후 조사를 지원하고 규정 및 조직의 정보 보존 요구 사항을 충족하기 위해 [할당: 기록 보존 정책에 따라 조직이 정의한 기간] 동안 감사 기록을 보관합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
AU-12(a)(c)	정보 시스템: a. AU-2 a. [할당: 조직 정의 정보 시스템 구성 요소]에서 정의된 감사 가능 이벤트에 대한 감사 기록 생성 기능을 제공합니다. 정보 시스템 c: AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-12(a)(c)	정보 시스템: a. AU-2 a. [할당: 조직 정의 정보 시스템 구성 요소]에서 정의된 감사 가능 이벤트에 대한 감사 기록 생성 기능을 제공합니다. 정보 시스템 c: AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-12(a)(c)	정보 시스템: a. AU-2 a. [할당: 조직 정의 정보 시스템 구성 요소]에서 정의된 감사 가능 이벤트에 대한 감사 기록 생성 기능을 제공합니다. 정보 시스템 c: AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
AU-12(a)(c)	정보 시스템: a. AU-2 a. [할당: 조직 정의 정보 시스템 구성 요소]에서 정의된 감사 가능 이벤트에 대한 감사 기록 생성 기능을 제공합니다. 정보 시스템 c: AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-12(a)(c)	정보 시스템: a. AU-2 a. [할당: 조직 정의 정보 시스템 구성 요소]에서 정의된 감사 가능 이벤트에 대한 감사 기록 생성 기능을 제공합니다. 정보 시스템 c: AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	cloudtrail-enabled	AWS CloudTrail 는 Management Console 작업 및 API 호출을 기록 AWS 하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-12(a)(c)	정보 시스템: a. AU-2 a. [할당: 조직 정의 정보 시스템 구성 요소]에서 정의된 감사 가능 이벤트에 대한 감사 기록 생성 기능을 제공합니다. 정보 시스템 c: AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-12(a)(c)	정보 시스템: a. AU-2 a. [할당: 조직 정의 정보 시스템 구성 요소]에서 정의된 감사 가능 이벤트에 대한 감사 기록 생성 기능을 제공합니다. 정보 시스템 c: AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail 는 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든에서 S3 버킷 AWS 리전으로 로그 파일을 전송합니다. 또한 AWS 에서 새 리전을 시작하면 CloudTrail은 새 리전에 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-12(a)(c)	정보 시스템: a. AU-2 a. [할당: 조직 정의 정보 시스템 구성 요소]에서 정의된 감사 가능 이벤트에 대한 감사 기록 생성 기능을 제공합니다. 정보 시스템 c: AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-12(a)(c)	정보 시스템: a. AU-2 a. [할당: 조직 정의 정보 시스템 구성 요소]에서 정의된 감사 가능 이벤트에 대한 감사 기록 생성 기능을 제공합니다. 정보 시스템 c: AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-12(a)(c)	정보 시스템: a. AU-2 a. [할당: 조직 정의 정보 시스템 구성 요소]에서 정의된 감사 가능 이벤트에 대한 감사 기록 생성 기능을 제공합니다. 정보 시스템 c: AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
AU-12(a)(c)	정보 시스템: a. AU-2 a. [할당: 조직 정의 정보 시스템 구성 요소]에서 정의된 감사 가능 이벤트에 대한 감사 기록 생성 기능을 제공합니다. 정보 시스템 c: AU-3에 정의된 내용과 함께 AU-2 d에 정의된 이벤트에 대한 감사 기록을 생성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CA-7(a)(b)	조직 a: 지속적 모니터링 전략을 개발하고 다음을 포함하는 지속적 모니터링 프로그램을 구현합니다. 모니터링할 [할당: 조직 정의 지표] 설정. 조직 b: 모니터링을 위한 [할당: 조직 정의 주파수] 설정 및 이러한 모니터링을 지원하는 평가를 위한 [할당: 조직 정의 빈도] 설정	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
CM-2	조직은 구성 제어 하에 정보 시스템의 현재 기본 구성을 개발, 문서화 및 유지 관리합니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 AWS CloudTrail확인하여에 대한 AWS 권장 보안 모범 사례를 사용하는 데 도움이 됩니다. 여기에는 여러 리전 AWS CloudTrail 에서 로그 암호화, 로그 검증 및 활성화 사용이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CM-7(a)	조직: a. 필수 기능만 제공하도록 정보 시스템을 구성합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CM-7(a)	조직: a. 필수 기능만 제공하도록 정보 시스템을 구성합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CM-8(1)	조직은 구성 요소 설치, 제거 및 정보 시스템 업데이트의 필수 부분으로 정보 시스템 구성 요소 인벤토리를 업데이트합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CM-8(3)(a)	조직 a: 자동화된 메커니즘을 [과제: 조직에서 정의한 빈도]로 사용하여 정보 시스템 내에 승인되지 않은 하드웨어, 소프트웨어 및 펌웨어 구성 요소가 있는지 탐지합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CM-8(3)(a)	조직 a: 자동화된 메커니즘을 [과제: 조직에서 정의한 빈도]로 사용하여 정보 시스템 내에 승인되지 않은 하드웨어, 소프트웨어 및 펌웨어 구성 요소가 있는지 탐지합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
CM-8(3)(a)	조직 a: 자동화된 메커니즘을 [과제: 조직에서 정의한 빈도]로 사용하여 정보 시스템 내에 승인되지 않은 하드웨어, 소프트웨어 및 펌웨어 구성 요소가 있는지 탐지합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9(b)	조직: b. 정보 시스템에 포함된 시스템 수준 정보의 백업을 [할당: 복구 시간 및 복구 지점 목표에 부합하는 조직 정의 빈도]로 수행합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
CP-10	조직은 중단, 손상 또는 장애 발생 후 정보 시스템을 알려진 상태로 복구 및 재구성할 수 있도록 지원합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
IA-2	정보 시스템은 조직 사용자(또는 조직 사용자를 대신하여 활동하는 프로세스)를 고유하게 식별하고 인증합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 CIS(인터넷 보안 센터) AWS 파운데이션 벤치마크의 암호 강도에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS Config 규칙	지침
			조직의 정책을 반영해야 합니다.
IA-2(1)(11)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다. (11) 정보 시스템은 권한 있는 계정 및 권한이 없는 계정에 대한 원격 액세스를 위한 다중 인증을 구현합니다. 인증 요소 중 하나는 액세스 권한을 얻는 시스템과 분리된 장치에서 제공하고 해당 장치는 [할당: 조직이 정의한 메커니즘 강도 요구 사항]을 충족합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
IA-2(1)(11)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다. (11) 정보 시스템은 권한 있는 계정 및 권한이 없는 계정에 대한 원격 액세스를 위한 다중 인증을 구현합니다. 인증 요소 중 하나는 액세스 권한을 얻는 시스템과 분리된 장치에서 제공하고 해당 장치는 [할당: 조직이 정의한 메커니즘 강도 요구 사항]을 충족합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
IA-2(1)(2)(11)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다. (2) 정보 시스템은 권한이 없는 계정에 대한 네트워크 액세스를 위해 다중 인증을 구현합니다. (11) 정보 시스템은 권한 있는 계정 및 권한이 없는 계정에 대한 원격 액세스를 위한 다중 인증을 구현합니다. 인증 요소 중 하나는 액세스 권한을 얻는 시스템과 분리된 장치에서 제공하고 해당 장치는 [할당: 조직이 정의한 메커니즘 강도 요구 사항]을 충족합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
IA-2(1)(2)(11)	(1) 정보 시스템은 권한 있는 계정에 대한 네트워크 액세스를 위한 다중 인증을 구현합니다. (2) 정보 시스템은 권한이 없는 계정에 대한 네트워크 액세스를 위해 다중 인증을 구현합니다. (11) 정보 시스템은 권한 있는 계정 및 권한이 없는 계정에 대한 원격 액세스를 위한 다중 인증을 구현합니다. 인증 요소 중 하나는 액세스 권한을 얻는 시스템과 분리된 장치에서 제공하고 해당 장치는 [할당: 조직이 정의한 메커니즘 강도 요구 사항]을 충족합니다.	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS Config 규칙	지침
IA-5(1)(a)(d)(e)	암호 기반 인증을 위한 정보 시스템: a. a. 최소한의 암호 복잡성 수준 강제[할당: 각 유형에 대한 최소 요구 사항을 포함하여 대소문자 구분, 문자 수, 대소문자 혼합, 숫자 및 특수 문자에 대한 조직에서 정의한 요구 사항] d. 암호의 최소 및 최대 수명 제한 적용[할당: 조직에서 정의한 최소 수명 및 최대 수명] e. [할당: 조직에서 정의한 번호] 세대 동안 암호 재사용 금지	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 CIS(인터넷 보안 센터) AWS 파운데이션 벤치마크의 암호 강도에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS Config 규칙	지침
			조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
IA-5(4)	조직에서는 자동화된 도구를 사용하여 암호 인증자가 [할당: 조직에서 정의한 요구 사항]을 충족할 만큼 충분히 강력한지 판단합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 CIS(인터넷 보안 센터) AWS 파운데이션 벤치마크의 암호 강도에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS Config 규칙	지침
			조직의 정책을 반영해야 합니다.
IA-5(7)	조직은 암호화되지 않은 정적 인증자가 애플리케이션이나 액세스 스크립트에 내장되거나 기능 키에 저장되지 않도록 합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
IR-4(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 처리 프로세스를 지원합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
IR-6(1)	조직은 자동화된 메커니즘을 사용하여 보안 인시던트를 보고하는 것을 지원합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
IR-7(1)	조직은 자동화된 메커니즘을 사용하여 인시던트 대응 관련 정보 및 지원의 가용성을 높입니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
RA-5	조직: a. 정보 시스템 및 호스팅된 애플리케이션에 대한 취약성 스캔을 [할당: 조직이 정의한 빈도 및/또는 조직이 정의한 프로세스에 따라 무작위로] 및 시스템/애플리케이션에 영향을 미칠 수 있는 새로운 취약성이 식별되고 보고되는 시점에 수행합니다. 조직 b: 다음에 대한 표준을 사용하여 도구 간의 상호 운용성을 촉진하고 취약성 관리 프로세스의 일부를 자동화하는 취약성 스캔 도구 및 기법을 사용합니다. 1. 플랫폼, 소프트웨어 결함 및 부적절한 구성 열거 2. 체크리스트 및 테스트 절차 형식 지정 3. 취약성 영향 측정 조직 c: 취약성 검사 보고서 및 보안 통제 평가 결과를 분석합니다. 조직 d: 조직의 위험 평가에 따라 정상적인 취약성을 [할당: 조직이 정의한 대응 시간] 내에 교정합니다. 조직 e: 취약성 검사 프로세스 및 보안 통제 평가에서 얻	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	은 정보를 [할당: 조직이 정의한 직원 또는 역할]과 공유하여 다른 정보 시스템의 유사한 취약성(예: 시스템적 약점 또는 결함)을 제거하는 데 도움을 줍니다.		

제어 ID	제어 설명	AWS Config 규칙	지침
RA-5	조직: a. 정보 시스템 및 호스팅된 애플리케이션에 대한 취약성 스캔을 [할당: 조직이 정의한 빈도 및/또는 조직이 정의한 프로세스에 따라 무작위로] 및 시스템/애플리케이션에 영향을 미칠 수 있는 새로운 취약성이 식별되고 보고되는 시점에 수행합니다. 조직 b: 다음에 대한 표준을 사용하여 도구 간의 상호 운용성을 촉진하고 취약성 관리 프로세스의 일부를 자동화하는 취약성 스캔 도구 및 기법을 사용합니다. 1. 플랫폼, 소프트웨어 결함 및 부적절한 구성 열거 2. 체크리스트 및 테스트 절차 형식 지정 3. 취약성 영향 측정 조직 c: 취약성 검사 보고서 및 보안 통제 평가 결과를 분석합니다. 조직 d: 조직의 위험 평가에 따라 정상적인 취약성을 [할당: 조직이 정의한 대응 시간] 내에 교정합니다. 조직 e: 취약성 검사 프로세스 및 보안 통제 평가에서 얻	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
	은 정보를 [할당: 조직이 정의한 직원 또는 역할]과 공유하여 다른 정보 시스템의 유사한 취약성(예: 시스템적 약점 또는 결함)을 제거하는 데 도움을 줍니다.		
SA-3(a)	조직: a. 정보 보안 고려 사항을 포함하는 [할당: 조직이 정의한 시스템 개발 수명 주기]를 사용하여 정보 시스템을 관리합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SA-3(a)	조직: a. 정보 보안 고려 사항을 포함하는 [할당: 조직이 정의한 시스템 개발 수명 주기]를 사용하여 정보 시스템을 관리합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
SA-3(a)	조직: a. 정보 보안 고려 사항을 포함하는 [할당: 조직이 정의한 시스템 개발 수명 주기]를 사용하여 정보 시스템을 관리합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 보안 인증 정보가 포함되지 않도록 합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. a. 시스템, 구성 요소 또는 서비스의 [선택(하나 이상): 설계, 개발, 구현, 운영] 중 구성 관리 수행 b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. a. 시스템, 구성 요소 또는 서비스의 [선택(하나 이상): 설계, 개발, 구현, 운영] 중 구성 관리 수행 b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. a. 시스템, 구성 요소 또는 서비스의 [선택(하나 이상): 설계, 개발, 구현, 운영] 중 구성 관리 수행 b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SA-10	조직은 정보 시스템, 시스템 구성 요소 또는 정보 시스템 서비스 개발자에게 다음을 요구합니다. a. 시스템, 구성 요소 또는 서비스의 [선택(하나 이상): 설계, 개발, 구현, 운영] 중 구성 관리 수행 b. [할당: 구성 관리 중인 조직 정의 구성 항목]에 대한 변경 사항의 무결성을 문서화, 관리 및 제어 c. 시스템, 구성 요소 또는 서비스에 대해 조직에서 승인한 변경 사항만 구현 d. 시스템, 구성 요소 또는 서비스에 대한 승인된 변경 사항과 그러한 변경으로 인한 잠재적 보안 영향 문서화 시스템, 구성 요소 또는 서비스 내의 보안 결함 및 결함 해결을 추적하고 결과를 [할당: 조직 정의 담당자]에게 보고.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
SC-2	정보 시스템은 사용자 기능(사용자 인터페이스 서비스 포함)을 정보 시스템 관리 기능과 분리합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-4	정보 시스템은 공유 시스템 리소스에서 승인되지 않거나 의도하지 않은 정보 전송을 방지합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기 및 쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-5	정보 시스템은 [할당: 조직이 정의한 보안 보호 장치]를 사용하여 [할당: 조직에서 정의한 유형의 서비스 거부 공격 또는 해당 정보의 출처에 대한 참조]와 같은 유형의 서비스 거부 공격으로부터 보호하거나 그 영향을 제한합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	s3-account-level-public-access-blocks	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7	정보 시스템: a. a. 시스템 외부 경계 및 시스템 내 주요 내부 경계에서의 통신을 모니터링하고 제어합니다. b. [선택: 물리적으로, 논리적으로] 내부 조직 네트워크와 분리된 공개적으로 액세스할 수 있는 시스템 구성 요소를 위한 서브네트워크를 구현합니다. c. 조직 보안 아키텍처에 따라 정렬된 경계 보호 장치로 구성된 관리형 인터페이스를 통해서만 외부 네트워크 또는 정보 시스템에 연결합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-account-level-public-access-blocks	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-7(3)	정보 시스템에 대한 외부 네트워크 연결 수를 제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
SC-8	정보 시스템은 전송된 정보의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-8	정보 시스템은 전송된 정보의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	정보 시스템은 전송된 정보의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	정보 시스템은 전송된 정보의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-8	정보 시스템은 전송된 정보의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	정보 시스템은 전송된 정보의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-8	정보 시스템은 전송된 정보의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-8(1)	정보 시스템은 [할당: 조직이 정의한 대체 물리적 보호 장치]에 의해 달리 보호되지 않는 한 전송 중에 [선택(하나 이상): 정보의 무단 공개 방지, 정보 변경 감지]를 위한 암호화 메커니즘을 구현합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-12	조직은 [할당: 키 생성, 배포, 저장, 액세스 및 폐기에 대한 조직이 정의한 요구 사항]에 따라 정보 시스템 내에서 사용되는 필수 암호화를 위한 암호화 키를 설정하고 관리합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암 호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-12	조직은 [할당: 키 생성, 배포, 저장, 액세스 및 폐기에 대한 조직이 정의한 요구 사항]에 따라 정보 시스템 내에서 사용되는 필수 암호화를 위한 암호화 키를 설정하고 관리합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
SC-12	조직은 [할당: 키 생성, 배포, 저장, 액세스 및 폐기에 대한 조직이 정의한 요구 사항]에 따라 정보 시스템 내에서 사용되는 필수 암호화를 위한 암호화 키를 설정하고 관리합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-13	정보 시스템은 해당 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 [할당: 조직에서 정의한 암호화 사용 및 각 용도에 필요한 암호화 유형]을 구현합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	정보 시스템은 관련 연방법, 행정 명령, 지침, 정책, 규정 및 표준에 따라 FIPS 검증 또는 NSA 승인 암호화를 구현합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23	정보 시스템은 통신 세션의 신뢰성을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	정보 시스템은 [할당: 조직이 정의한 저장된 정보]의 [선택(하나 이상): 기밀성, 무결성]을 보호합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-36	조직은 [할당: 조직이 정의한 처리 및 스토리지]를 여러 물리적 위치에 배포합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-36	조직은 [할당: 조직이 정의한 처리 및 스토리지]를 여러 물리적 위치에 배포합니다.	rds-cluster-multi-az-enabled	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SC-36	조직은 [할당: 조직이 정의한 처리 및 스토리지]를 여러 물리적 위치에 배포합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
SI-2(2)	조직은 자동화된 메커니즘을 [할당: 조직에서 정의한 빈도]를 사용하여 결함 수정과 관련된 정보 시스템 구성 요소의 상태를 결정합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-2(2)	조직은 자동화된 메커니즘을 [할당: 조직에서 정의한 빈도]를 사용하여 결함 수정과 관련된 정보 시스템 구성 요소의 상태를 결정합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-2(2)	조직은 자동화된 메커니즘을 [할당: 조직에서 정의한 빈도]를 사용하여 결함 수정과 관련된 정보 시스템 구성 요소의 상태를 결정합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
SI-4(1)	조직은 개별 침입 탐지 도구를 정보 시스템 전체의 침입 탐지 시스템에 연결하고 구성합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(2)	조직은 자동화된 도구를 사용하여 이벤트를 실시간에 가깝게 분석할 수 있습니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 [할당: 조직 정의 빈도]로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 [할당: 조직 정의 빈도]로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 [할당: 조직 정의 빈도]로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI-4(4)	정보 시스템은 인바운드 및 아웃바운드 통신 트래픽을 [할당: 조직 정의 빈도]로 모니터링하여 비정상적이거나 승인되지 않은 활동이나 조건을 확인합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI-4(5)	정보 시스템은 [할당: 조직이 정의한 침해 지표]의 침해 또는 잠재적 침해 징후가 발생할 경우 [할당: 조직에서 정의한 직원 또는 역할]에게 경보를 보냅니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(16)	조직은 정보 시스템 전반에 사용되는 모니터링 도구의 정보를 상호 연관시킵니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나, 보안을 손상시키거나, 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-4(a)(b)(c)	조직: a. 정보 시스템을 모니터링하여 다음을 탐지합니다. 1. [과제: 조직이 정의한 모니터링 목표]에 따른 공격 및 잠재적 공격의 지표. 2. 무단 로컬, 네트워크 및 원격 연결 조직 b: [과제: 조직에서 정의한 기법 및 방법]을 통해 정보 시스템의 무단 사용 식별. c. 조직 c: 모니터링 장치 배치. 1) 조직이 결정한 필수 정보를 수집하기 위해 정보 시스템 내에 전략적으로 배치 2) 조직이 관심을 갖는 특정 유형의 거래를 추적하기 위해 시스템 내 애드혹 위치에 배치	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-7	조직은 무결성 검증 도구를 사용하여 [할당: 조직 정의 소프트웨어, 펌웨어 및 정보]의 무단 변경을 탐지합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-7(1)	정보 시스템은 [할당: 조직이 정의한 소프트웨어, 펌웨어 및 정보] [선택(하나 이상): 시작 시, [할당: 조직이 정의한 전환 상태 또는 보안 관련 이벤트 시] 또는 [할당: 조직이 정의한 빈도]]에 따라 무결성 검사를 수행합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
SI-7(1)	정보 시스템은 [할당: 조직이 정의한 소프트웨어, 펌웨어 및 정보] [선택(하나 이상): 시작 시, [할당: 조직이 정의한 전환 상태 또는 보안 관련 이벤트 시] 또는 [할당: 조직이 정의한 빈도]]에 따라 무결성 검사를 수행합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-7(1)	정보 시스템은 [할당: 조직이 정의한 소프트웨어, 펌웨어 및 정보] [선택(하나 이상): 시작 시, [할당: 조직이 정의한 전환 상태 또는 보안 관련 이벤트 시] 또는 [할당: 조직이 정의한 빈도]]에 따라 무결성 검사를 수행합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS Config 규칙	지침
SI-12	조직은 관련 연방법, 행정 명령, 지침, 정책, 규정, 표준 및 운영 요구 사항에 따라 정보 시스템 내의 정보와 시스템에서 출력되는 정보를 처리하고 유지합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

템플릿

템플릿은 GitHub: NIST 800-53 rev 4 운영 모범 사례에서 확인할 수 있습니다.

NIST 800-53 rev 5 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 NIST 800-53과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 NIST 800-53 제어와 관련이 있습니다. NIST 800-53 제어는 여러 구성 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	계정 관리 | 자동화된 감사 작업	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon

제어 ID	제어 설명	AWS 구성 규칙	지침
			CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AC-2(4)	계정 관리 | 자동화된 감사 작업	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	계정 관리 | 자동화된 감사 작업	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AC-2(4)	계정 관리 | 자동화된 감사 작업	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	계정 관리 | 자동화된 감사 작업	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AC-2(4)	계정 관리 | 자동화된 감사 작업	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	계정 관리 | 자동화된 감사 작업	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	계정 관리 | 자동화된 감사 작업	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2(4)	계정 관리 | 자동화된 감사 작업	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AC-2(12)	계정 관리 | 이례적 사용에 대한 계정 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-2	계정 관리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-2	계정 관리	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-2	계정 관리	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3(15)	액세스 통제 | 임의 및 필수 액세스 제어	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
AC-3	액세스 통제	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
AC-3	액세스 통제	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
AC-3	액세스 통제	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-3	액세스 통제	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-3	액세스 통제	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	액세스 통제	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	액세스 통제	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
AC-3	액세스 통제	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-3	액세스 통제	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
AC-3	액세스 통제	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-3	액세스 통제	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC-3	액세스 통제	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-3	액세스 통제	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-3	액세스 통제	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AC-4(26)	정보 흐름 통제 | 감사 필터링 작업	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5	업무 분리	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.
AC-5	업무 분리	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
AC-5	업무 분리	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5	업무 분리	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5	업무 분리	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-5	업무 분리	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-6(2)	최소 권한 | 비보안 기능에 대한 비권한 액세스	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(2)	최소 권한 | 비보안 기능에 대한 비권한 액세스	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-6(2)	최소 권한 | 비보안 기능에 대한 비권한 액세스	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(3)	최소 권한 | 권한이 있는 명령에 대한 네트워크 액세스	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
AC-6(3)	최소 권한 | 권한이 있는 명령에 대한 네트워크 액세스	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(3)	최소 권한 | 권한이 있는 명령에 대한 네트워크 액세스	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(3)	최소 권한 | 권한이 있는 명령에 대한 네트워크 액세스	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(3)	최소 권한 | 권한이 있는 명령에 대한 네트워크 액세스	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-6(3)	최소 권한 | 권한이 있는 명령에 대한 네트워크 액세스	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	최소 권한 | 권한이 있는 함수의 로그 사용	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	최소 권한 | 권한이 있는 함수의 로그 사용	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	최소 권한 | 권한이 있는 함수의 로그 사용	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AC-6(9)	최소 권한 | 권한이 있는 함수의 로그 사용	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	최소 권한 | 권한이 있는 함수의 로그 사용	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AC-6(9)	최소 권한 | 권한이 있는 함수의 로그 사용	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	최소 권한 | 권한이 있는 함수의 로그 사용	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	최소 권한 | 권한이 있는 함수의 로그 사용	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(9)	최소 권한 | 권한이 있는 함수의 로그 사용	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AC-6(10)	최소 권한 | 권한이 없는 사용자의 권한이 있는 기능 실행 금지	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-6(10)	최소 권한 | 권한이 없는 사용자의 권한이 있는 기능 실행 금지	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
AC-6(10)	최소 권한 | 권한이 없는 사용자의 권한이 있는 기능 실행 금지	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(2)	원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
AC-17(2)	원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC-17(2)	원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(2)	원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AC-17(2)	원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-17(2)	원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
AC-17(2)	원격 액세스 | 암호화를 사용한 기밀성 및 무결성 보호	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
AC-21	정보 공유	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21	정보 공유	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21	정보 공유	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21	정보 공유	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
AC-21	정보 공유	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
AC-21	정보 공유	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
AC-21	정보 공유	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AC-21	정보 공유	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
AU-2	이벤트 로깅	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	이벤트 로깅	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	이벤트 로깅	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AU-2	이벤트 로깅	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	이벤트 로깅	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
AU-2	이벤트 로깅	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-2	이벤트 로깅	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	이벤트 로깅	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-2	이벤트 로깅	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	이벤트 로깅	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	이벤트 로깅	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-2	이벤트 로깅	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-2	이벤트 로깅	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AU-3	감사 기록 내용	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-3	감사 기록 내용	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-3	감사 기록 내용	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AU-3	감사 기록 내용	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-3	감사 기록 내용	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-3	감사 기록 내용	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)	감사 기록 검토, 분석 및 보고 | 자동화된 프로세스 통합	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-6(1)	감사 기록 검토, 분석 및 보고 | 자동화된 프로세스 통합	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)	감사 기록 검토, 분석 및 보고 | 자동화된 프로세스 통합	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(1)	감사 기록 검토, 분석 및 보고 | 자동화된 프로세스 통합	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-6(3)	감사 기록 검토, 분석 및 보고 | 감사 기록 리포지토리의 상관 관계 분석	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-6(4)	감사 기록 검토, 분석 및 보고 | 중앙 검토 및 분석	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(5)	감사 기록 검토, 분석 및 보고 | 감사 기록의 통합 분석	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-6(5)	감사 기록 검토, 분석 및 보고 | 감사 기록의 통합 분석	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(5)	감사 기록 검토, 분석 및 보고 | 감사 기록의 통합 분석	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-6(5)	감사 기록 검토, 분석 및 보고 | 감사 기록의 통합 분석	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
AU-7(1)	감사 기록 축소 및 보고서 생성 | 자동 처리	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9(2)	감사 정보 보호 | 별도의 물리적 시스템 또는 구성 요소에 저장	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
AU-9(2)	감사 정보 보호 | 별도의 물리적 시스템 또는 구성 요소에 저장	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9(2)	감사 정보 보호 | 별도의 물리적 시스템 또는 구성 요소에 저장	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
AU-9(7)	감사 정보 보호 | 다른 운영 체제의 구성 요소에 저장	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9	감사 정보 보호	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
AU-9	감사 정보 보호	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-9	감사 정보 보호	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-9	감사 정보 보호	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
AU-9	감사 정보 보호	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-10	부인 방지	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-10	부인 방지	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-10	부인 방지	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AU-10	부인 방지	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-10	부인 방지	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
AU-10	부인 방지	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-10	부인 방지	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-10	부인 방지	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
AU-10	부인 방지	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-10	부인 방지	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-10	부인 방지	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-10	부인 방지	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-12	감사 기록 생성	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 기록 생성	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 기록 생성	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
AU-12	감사 기록 생성	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 기록 생성	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
AU-12	감사 기록 생성	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
AU-12	감사 기록 생성	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 기록 생성	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
AU-12	감사 기록 생성	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 기록 생성	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 기록 생성	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-12	감사 기록 생성	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
AU-12	감사 기록 생성	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AU-14(1)	세션 감사 | 시스템 시작	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CA-7	지속적인 모니터링	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
CA-7	지속적인 모니터링	s3-event-notifications-enabled	Amazon S3 이벤트 알림은 버킷 객체가 우발적이거나 의도적으로 수정된 경우 관련 담당자에게 알릴 수 있습니다. 알림의 예로는 새 객체 생성, 객체 제거, 객체 복원, 분실 및 복제된 객체 등이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
CA-7	지속적인 모니터링	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 확장 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
CA-7	지속적인 모니터링	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
CA-7	지속적인 모니터링	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
CA-7	지속적인 모니터링	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-7	지속적인 모니터링	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
CA-7	지속적인 모니터링	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	rds-instance-default-admin-check	기본 사용자 이름은 공개적으로 알려져 있으므로 기본 사용자 이름을 변경하면 Amazon Relational Database Service(RDS) 데이터베이스 클러스터의 공격 표면을 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	redshift-default-admin-check	기본 사용자 이름은 공개적으로 알려져 있으므로 기본 사용자 이름을 변경하면 Amazon Redshift 클러스터의 공격 표면을 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CA-9(1)	내부 시스템 연결 | 규정 준수 검사	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2(2)	기본 구성 | 정확성 및 최신성을 위한 자동화 지원	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2(2)	기본 구성 | 정확성 및 최신성을 위한 자동화 지원	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
CM-2(2)	기본 구성 | 정확성 및 최신성을 위한 자동화 지원	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2(2)	기본 구성 | 정확성 및 최신성을 위한 자동화 지원	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
CM-2(2)	기본 구성 | 정확성 및 최신성을 위한 자동화 지원	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2(2)	기본 구성 | 정확성 및 최신성을 위한 자동화 지원	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
CM-2	기본 구성	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	기본 구성	rds-instance-default-admin-check	기본 사용자 이름은 공개적으로 알려져 있으므로 기본 사용자 이름을 변경하면 Amazon Relational Database Service(RDS) 데이터베이스 클러스터의 공격 표면을 줄이는 데 도움이 됩니다.
CM-2	기본 구성	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	기본 구성	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
CM-2	기본 구성	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	기본 구성	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
CM-2	기본 구성	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	기본 구성	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
CM-2	기본 구성	redshift-default-admin-check	기본 사용자 이름은 공개적으로 알려져 있으므로 기본 사용자 이름을 변경하면 Amazon Redshift 클러스터의 공격 표면을 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-2	기본 구성	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
CM-3(6)	구성 변경 제어 | 암호화 관리	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-3(6)	구성 변경 제어 | 암호화 관리	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
CM-3(6)	구성 변경 제어 | 암호화 관리	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CM-3(6)	구성 변경 제어 | 암호화 관리	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-3(6)	구성 변경 제어 | 암호화 관리	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CM-3(6)	구성 변경 제어 | 암호화 관리	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CM-3(6)	구성 변경 제어 | 암호화 관리	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-3(6)	구성 변경 제어 | 암호화 관리	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CM-3(6)	구성 변경 제어 | 암호화 관리	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
CM-3(6)	구성 변경 제어 | 암호화 관리	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-3(6)	구성 변경 제어 | 암호화 관리	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
CM-3(6)	구성 변경 제어 | 암호화 관리	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
CM-3(6)	구성 변경 제어 | 암호화 관리	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-3(6)	구성 변경 제어 | 암호화 관리	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
CM-3(6)	구성 변경 제어 | 암호화 관리	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-3(6)	구성 변경 제어 | 암호화 관리	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-3(6)	구성 변경 제어 | 암호화 관리	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CM-3(6)	구성 변경 제어 | 암호화 관리	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-3(6)	구성 변경 제어 | 암호화 관리	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CM-3(6)	구성 변경 제어 | 암호화 관리	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-3	구성 변경 제어	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
CM-3	구성 변경 제어	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-7	최소 기능	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
CM-7	최소 기능	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-7	최소 기능	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(1)	시스템 구성 요소 인벤토리 | 설치 및 제거 중 업데이트	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(1)	시스템 구성 요소 인벤토리 | 설치 및 제거 중 업데이트	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(2)	시스템 구성 요소 인벤토리 | 자동 유지 관리	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(3)	시스템 구성 요소 인벤토리 | 자동화된 무단 구성 요소 탐지	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(3)	시스템 구성 요소 인벤토리 | 자동화된 무단 구성 요소 탐지	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
CM-8(3)	시스템 구성 요소 인벤토리 | 자동화된 무단 구성 요소 탐지	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8(3)	시스템 구성 요소 인벤토리 | 자동화된 무단 구성 요소 탐지	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
CM-8	시스템 구성 요소 인벤토리	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CM-8	시스템 구성 요소 인벤토리	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-2(2)	비상 계획 | 용량 계획	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-2(2)	비상 계획 | 용량 계획	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CP-6(1)	대체 스토리지 사이트 | 기본 사이트와 분리	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(1)	대체 스토리지 사이트 | 기본 사이트와 분리	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-6(1)	대체 스토리지 사이트 | 기본 사이트와 분리	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(1)	대체 스토리지 사이트 | 기본 사이트와 분리	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
CP-6(1)	대체 스토리지 사이트 | 기본 사이트와 분리	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(1)	대체 스토리지 사이트 | 기본 사이트와 분리	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
CP-6(1)	대체 스토리지 사이트 | 기본 사이트와 분리	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(1)	대체 스토리지 사이트 | 기본 사이트와 분리	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6(2)	대체 스토리지 사이트 | 복구 시간 및 복구 시점 목표	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6	대체 스토리지 사이트	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-6	대체 스토리지 사이트	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6	대체 스토리지 사이트	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-6	대체 스토리지 사이트	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6	대체 스토리지 사이트	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CP-6	대체 스토리지 사이트	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-6	대체 스토리지 사이트	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-6	대체 스토리지 사이트	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	시스템 백업	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9	시스템 백업	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	시스템 백업	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-9	시스템 백업	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	시스템 백업	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
CP-9	시스템 백업	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	시스템 백업	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
CP-9	시스템 백업	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	시스템 백업	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 실패할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	시스템 백업	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-9	시스템 백업	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-9	시스템 백업	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	시스템 복구 및 재구성	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	시스템 복구 및 재구성	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	시스템 복구 및 재구성	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
CP-10	시스템 복구 및 재구성	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	시스템 복구 및 재구성	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
CP-10	시스템 복구 및 재구성	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	시스템 복구 및 재구성	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
CP-10	시스템 복구 및 재구성	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	시스템 복구 및 재구성	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
CP-10	시스템 복구 및 재구성	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	시스템 복구 및 재구성	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	시스템 복구 및 재구성	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	시스템 복구 및 재구성	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
CP-10	시스템 복구 및 재구성	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CP-10	시스템 복구 및 재구성	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(1)	식별 및 인증(기관 사용자) | 권한 있는 계정에 대한 다중 인증	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
IA-2(1)	식별 및 인증(기관 사용자) | 권한 있는 계정에 대한 다중 인증	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(1)	식별 및 인증(기관 사용자) | 권한 있는 계정에 대한 다중 인증	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA-2(1)	식별 및 인증(기관 사용자) | 권한 있는 계정에 대한 다중 인증	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(2)	식별 및 인증(기관 사용자) | 권한이 없는 계정에 대한 다중 인증	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
IA-2(2)	식별 및 인증(기관 사용자) | 권한이 없는 계정에 대한 다중 인증	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(2)	식별 및 인증(기관 사용자) | 권한이 없는 계정에 대한 다중 인증	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA-2(2)	식별 및 인증(기관 사용자) | 권한이 없는 계정에 대한 다중 인증	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(6)	식별 및 인증(기관 사용자) | 계정 액세스 - 별도의 장치	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
IA-2(6)	식별 및 인증(기관 사용자) | 계정 액세스 - 별도의 장치	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(6)	식별 및 인증(기관 사용자) | 계정 액세스 - 별도의 장치	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA-2(6)	식별 및 인증(기관 사용자) | 계정 액세스 - 별도의 장치	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(8)	식별 및 인증(조직 사용자) | 계정 액세스 - 재실행 방지	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
IA-2(8)	식별 및 인증(조직 사용자) | 계정 액세스 - 재실행 방지	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-2(8)	식별 및 인증(조직 사용자) | 계정 액세스 - 재실행 방지	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
IA-2(8)	식별 및 인증(조직 사용자) | 계정 액세스 - 재실행 방지	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-5(1)	인증자 관리 | 암호 기반 인증	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
IA-5(1)	인증자 관리 | 암호 기반 인증	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
IA-5(1)	인증자 관리 | 암호 기반 인증	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-5(1)	인증자 관리 | 암호 기반 인증	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
IA-5(1)	인증자 관리 | 암호 기반 인증	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-5(1)	인증자 관리 | 암호 기반 인증	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IA-5(1)	인증자 관리 | 암호 기반 인증	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
IA-5(1)	인증자 관리 | 암호 기반 인증	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
IA-5(7)	인증자 관리 | 암호화된 정적 인증자만 사용	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4(1)	인시던트 처리 | 자동화된 인시던트 처리 프로세스	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
IR-4(5)	인시던트 처리 | 시스템 자동 비활성화	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RA-3(4)	위험 평가 | 예측 사이버 분석	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SA-3	시스템 개발 수명 주기	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-3	시스템 개발 수명 주기	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
SA-8(19)	보안 및 개인정보 보호 엔지니어링 원칙 | 지속적 보호	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-8(21)	보안 및 개인정보 보호 엔지니어링 원칙 | 자체 분석	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SA-8(22)	보안 및 개인정보 보호 엔지니어링 원칙 | 책임 및 추적 가능성	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-8(25)	보안 및 개인정보 보호 엔지니어링 원칙 | 경제 안보	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SA-11(1)	개발자 테스트 및 평가 | 정적 코드 분석	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-11(6)	개발자 테스트 및 평가 | 공격 표면 검토	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SA-15(2)	개발 프로세스, 표준 및 도구 | 보안 및 개인정보 추적 도구	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-15(2)	개발 프로세스, 표준 및 도구 | 보안 및 개인 정보 추적 도구	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SA-15(8)	개발 프로세스, 표준 및 도구 | 위협 및 취약성 정보의 재사용	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SA-15(8)	개발 프로세스, 표준 및 도구 | 위협 및 취약성 정보의 재사용	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SC-5(1)	서비스 거부 보호 | 다른 시스템 공격 권한 제한	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(2)	서비스 거부 보호 | 용량, 대역폭 및 이중화	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-5(3)	서비스 거부 보호 | 탐지 및 모니터링	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SC-5	서비스 거부 보호	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
SC-7(3)	경계 보호 | 액세스 포인트	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	경계 보호 | 액세스 포인트	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	경계 보호 | 액세스 포인트	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	경계 보호 | 액세스 포인트	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(3)	경계 보호 | 액세스 포인트	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SC-7(3)	경계 보호 | 액세스 포인트	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7(3)	경계 보호 | 액세스 포인트	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(3)	경계 보호 | 액세스 포인트	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
SC-7(4)	경계 보호 | 외부 통신 서비스	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(4)	경계 보호 | 외부 통신 서비스	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(5)	경계 보호 | 기본 거부 - 예외별 허용	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(5)	경계 보호 | 기본 거부 - 예외별 허용	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(5)	경계 보호 | 기본 거부 - 예외별 허용	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(5)	경계 보호 | 기본 거부 - 예외별 허용	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(9)	경계 보호 | 위협적인 발신 통신 트래픽 제한	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
SC-7(10)	경계 보호 | 유출 방지	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(10)	경계 보호 | 유출 방지	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
SC-7(10)	경계 보호 | 유출 방지	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-7(10)	경계 보호 | 유출 방지	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(10)	경계 보호 | 유출 방지	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
SC-7(10)	경계 보호 | 유출 방지	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-7(10)	경계 보호 | 유출 방지	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(10)	경계 보호 | 유출 방지	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-7(10)	경계 보호 | 유출 방지	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(10)	경계 보호 | 유출 방지	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(10)	경계 보호 | 유출 방지	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(10)	경계 보호 | 유출 방지	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-7(10)	경계 보호 | 유출 방지	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(10)	경계 보호 | 유출 방지	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-7(10)	경계 보호 | 유출 방지	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(10)	경계 보호 | 유출 방지	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-7(10)	경계 보호 | 유출 방지	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(10)	경계 보호 | 유출 방지	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(11)	경계 보호 | 수신 통신 트래픽 제한	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(16)	경계 보호 | 시스템 구성 요소 발견 방지	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7(21)	경계 보호 | 시스템 구성 요소 격리	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
SC-7	경계 보호	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
SC-7	경계 보호	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서에는 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
SC-7	경계 보호	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7	경계 보호	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7	경계 보호	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7	경계 보호	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7	경계 보호	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
SC-7	경계 보호	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
SC-7	경계 보호	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
SC-7	경계 보호	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
SC-7	경계 보호	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-7	경계 보호	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(1)	전송 기밀성 및 무결성 | 암호화 보호	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	전송 기밀성 및 무결성 | 암호화 보호	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(1)	전송 기밀성 및 무결성 | 암호화 보호	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	전송 기밀성 및 무결성 | 암호화 보호	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
SC-8(1)	전송 기밀성 및 무결성 | 암호화 보호	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(1)	전송 기밀성 및 무결성 | 암호화 보호	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(1)	전송 기밀성 및 무결성 | 암호화 보호	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(1)	전송 기밀성 및 무결성 | 암호화 보호	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-8(1)	전송 기밀성 및 무결성 | 암호화 보호	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(1)	전송 기밀성 및 무결성 | 암호화 보호	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(2)	전송 기밀성 및 무결성 | 전송 전 및 전송 후 처리	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(2)	전송 기밀성 및 무결성 | 전송 전 및 전송 후 처리	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(2)	전송 기밀성 및 무결성 | 전송 전 및 전송 후 처리	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
SC-8(2)	전송 기밀성 및 무결성 | 전송 전 및 전송 후 처리	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(2)	전송 기밀성 및 무결성 | 전송 전 및 전송 후 처리	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(2)	전송 기밀성 및 무결성 | 전송 전 및 전송 후 처리	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(2)	전송 기밀성 및 무결성 | 전송 전 및 전송 후 처리	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-8(2)	전송 기밀성 및 무결성 | 전송 전 및 전송 후 처리	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8(2)	전송 기밀성 및 무결성 | 전송 전 및 전송 후 처리	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8(2)	전송 기밀성 및 무결성 | 전송 전 및 전송 후 처리	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8	전송 기밀성 및 무결성	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	전송 기밀성 및 무결성	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8	전송 기밀성 및 무결성	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	전송 기밀성 및 무결성	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
SC-8	전송 기밀성 및 무결성	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8	전송 기밀성 및 무결성	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-8	전송 기밀성 및 무결성	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8	전송 기밀성 및 무결성	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-8	전송 기밀성 및 무결성	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-8	전송 기밀성 및 무결성	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-12(2)	암호화 키 설정 및 관리 | 대칭 키	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
SC-12(2)	암호화 키 설정 및 관리 | 대칭 키	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-12(3)	암호화 키 설정 및 관리 | 비대칭 키	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-12(3)	암호화 키 설정 및 관리 | 비대칭 키	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-12(3)	암호화 키 설정 및 관리 | 비대칭 키	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-12(3)	암호화 키 설정 및 관리 | 비대칭 키	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-12(3)	암호화 키 설정 및 관리 | 비대칭 키	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-12(3)	암호화 키 설정 및 관리 | 비대칭 키	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-12(3)	암호화 키 설정 및 관리 | 비대칭 키	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-12	암호화 키 설정 및 관리	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-12	암호화 키 설정 및 관리	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
SC-13	암호화 보호	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.
SC-13	암호화 보호	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	암호화 보호	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	암호화 보호	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.
SC-13	암호화 보호	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	암호화 보호	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	암호화 보호	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	암호화 보호	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SC-13	암호화 보호	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
SC-13	암호화 보호	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-13	암호화 보호	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
SC-13	암호화 보호	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-13	암호화 보호	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-13	암호화 보호	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	암호화 보호	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	암호화 보호	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-13	암호화 보호	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-13	암호화 보호	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23(3)	세션 인증 | 시스템에서 생성한 고유한 세션 식별자	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23(3)	세션 인증 | 시스템에서 생성한 고유한 세션 식별자	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23(3)	세션 인증 | 시스템에서 생성한 고유한 세션 식별자	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23(3)	세션 인증 | 시스템에서 생성한 고유한 세션 식별자	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23(3)	세션 인증 | 시스템에서 생성한 고유한 세션 식별자	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23(3)	세션 인증 | 시스템에서 생성한 고유한 세션 식별자	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
SC-23(3)	세션 인증 | 시스템에서 생성한 고유한 세션 식별자	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-23(3)	세션 인증 | 시스템에서 생성한 고유한 세션 식별자	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23(3)	세션 인증 | 시스템에서 생성한 고유한 세션 식별자	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23(5)	세션 인증 | 허용된 인증 기관	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23(5)	세션 인증 | 허용된 인증 기관	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-23	세션 인증	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23	세션 인증	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23	세션 인증	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
SC-23	세션 인증	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23	세션 인증	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23	세션 인증	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23	세션 인증	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SC-23	세션 인증	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-23	세션 인증	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-23	세션 인증	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(1)	저장된 정보 보호 | 암호화 보호	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(1)	저장된 정보 보호 | 암호화 보호	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
SC-28(1)	저장된 정보 보호 | 암호화 보호	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(1)	저장된 정보 보호 | 암호화 보호	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(1)	저장된 정보 보호 | 암호화 보호	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(1)	저장된 정보 보호 | 암호화 보호	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(1)	저장된 정보 보호 | 암호화 보호	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(1)	저장된 정보 보호 | 암호화 보호	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(1)	저장된 정보 보호 | 암호화 보호	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SC-28(1)	저장된 정보 보호 | 암호화 보호	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(1)	저장된 정보 보호 | 암호화 보호	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-28(1)	저장된 정보 보호 | 암호화 보호	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
SC-28(1)	저장된 정보 보호 | 암호화 보호	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(1)	저장된 정보 보호 | 암호화 보호	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
SC-28(1)	저장된 정보 보호 | 암호화 보호	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(1)	저장된 정보 보호 | 암호화 보호	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(1)	저장된 정보 보호 | 암호화 보호	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(1)	저장된 정보 보호 | 암호화 보호	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(1)	저장된 정보 보호 | 암호화 보호	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28(1)	저장된 정보 보호 | 암호화 보호	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28(3)	저장된 정보 보호 | 암호화 키	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
SC-28(3)	저장된 정보 보호 | 암호화 키	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
SC-28	저장된 정보 보호	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	저장된 정보 보호	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
SC-28	저장된 정보 보호	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	저장된 정보 보호	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	저장된 정보 보호	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	저장된 정보 보호	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	저장된 정보 보호	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	저장된 정보 보호	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	저장된 정보 보호	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SC-28	저장된 정보 보호	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	저장된 정보 보호	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SC-28	저장된 정보 보호	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
SC-28	저장된 정보 보호	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	저장된 정보 보호	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
SC-28	저장된 정보 보호	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	저장된 정보 보호	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	저장된 정보 보호	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	저장된 정보 보호	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-28	저장된 정보 보호	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SC-28	저장된 정보 보호	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-36(2)	분산 처리 및 저장 | 동기화	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
SC-36	분산 처리 및 스토리지	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-36	분산 처리 및 스토리지	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-36	분산 처리 및 스토리지	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SC-36	분산 처리 및 스토리지	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
SI-2(2)	결함 수정 | 자동 결함 수정 상태	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(2)	결함 수정 | 자동 결함 수정 상태	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(2)	결함 수정 | 자동 결함 수정 상태	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(3)	결함 수정 | 결함 수정 시간 및 시정 조치 벤치마크	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(3)	결함 수정 | 결함 수정 시간 및 시정 조치 벤치마크	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
SI-2(3)	결함 수정 | 결함 수정 시간 및 시정 조치 벤치마크	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(4)	결함 수정 | 자동화된 패치 관리 도구	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
SI-2(4)	결함 수정 | 자동화된 패치 관리 도구	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(4)	결함 수정 | 자동화된 패치 관리 도구	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(5)	결함 수정 | 소프트웨어 및 펌웨어 자동 업데이트	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
SI-2(5)	결함 수정 | 소프트웨어 및 펌웨어 자동 업데이트	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2(5)	결함 수정 | 소프트웨어 및 펌웨어 자동 업데이트	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
SI-2	결함 수정	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2	결함 수정	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2	결함 수정	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2	결함 수정	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 강화된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2	결함 수정	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2	결함 수정	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2	결함 수정	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
SI-2	결함 수정	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-2	결함 수정	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3(8)	악성 코드 보호 | 무단 명령 탐지	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3(8)	악성 코드 보호 | 무단 명령 탐지	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3(8)	악성 코드 보호 | 무단 명령 탐지	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
SI-3(8)	악성 코드 보호 | 무단 명령 탐지	s3-event-notifications-enabled	Amazon S3 이벤트 알림은 버킷 객체가 우발적이거나 의도적으로 수정된 경우 관련 담당자에게 알릴 수 있습니다. 알림의 예로는 새 객체 생성, 객체 제거, 객체 복원, 분실 및 복제된 객체 등이 있습니다.
SI-3(8)	악성 코드 보호 | 무단 명령 탐지	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3(8)	악성 코드 보호 | 무단 명령 탐지	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
SI-3(8)	악성 코드 보호 | 무단 명령 탐지	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3(8)	악성 코드 보호 | 무단 명령 탐지	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SI-3(8)	악성 코드 보호 | 무단 명령 탐지	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3(8)	악성 코드 보호 | 무단 명령 탐지	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-3(8)	악성 코드 보호 | 무단 명령 탐지	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
SI-4(1)	시스템 모니터링 | 시스템 전반의 침입 탐지 시스템	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(2)	시스템 모니터링 | 실시간 분석을 위한 자동화된 도구 및 메커니즘	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SI-4(4)	시스템 모니터링 | 인바운드 및 아웃바운드 통신 트래픽	s3-event-notifications-enabled	Amazon S3 이벤트 알림은 버킷 객체가 우발적이거나 의도적으로 수정된 경우 관련 담당자에게 알릴 수 있습니다. 알림의 예로는 새 객체 생성, 객체 제거, 객체 복원, 분실 및 복제된 객체 등이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(4)	시스템 모니터링 | 인바운드 및 아웃바운드 통신 트래픽	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(5)	시스템 모니터링 | 시스템 생성 알림	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI-4(5)	시스템 모니터링 | 시스템 생성 알림	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(5)	시스템 모니터링 | 시스템 생성 알림	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(12)	시스템 모니터링 | 조직에서 생성한 자동화된 알림	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(13)	시스템 모니터링 | 트래픽 및 이벤트 패턴 분석	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SI-4(20)	시스템 모니터링 | 권한이 있는 사용자	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(20)	시스템 모니터링 | 권한이 있는 사용자	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(20)	시스템 모니터링 | 권한이 있는 사용자	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
SI-4(20)	시스템 모니터링 | 권한이 있는 사용자	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(20)	시스템 모니터링 | 권한이 있는 사용자	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
SI-4(20)	시스템 모니터링 | 권한이 있는 사용자	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(20)	시스템 모니터링 | 권한이 있는 사용자	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(20)	시스템 모니터링 | 권한이 있는 사용자	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(20)	시스템 모니터링 | 권한이 있는 사용자	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
SI-4(22)	시스템 모니터링 | 무단 네트워크 서비스	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4(25)	시스템 모니터링 | 네트워크 트래픽 분석 최적화	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
SI-4	시스템 모니터링	s3-event-notifications-enabled	Amazon S3 이벤트 알림은 버킷 객체가 우발적이거나 의도적으로 수정된 경우 관련 담당자에게 알릴 수 있습니다. 알림의 예로는 새 객체 생성, 객체 제거, 객체 복원, 분실 및 복제된 객체 등이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4	시스템 모니터링	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-4	시스템 모니터링	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(1)	소프트웨어, 펌웨어 및 정보 무결성 | 무결성 검사	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(3)	소프트웨어, 펌웨어 및 정보 무결성 | 중앙에서 관리되는 무결성 도구	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(6)	소프트웨어, 펌웨어 및 정보 무결성 | 암호화 보호	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(7)	소프트웨어, 펌웨어 및 정보 무결성 | 탐지 및 대응 통합	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
SI-7(8)	소프트웨어, 펌웨어 및 정보 무결성 | 중요 이벤트에 대한 감사 기능	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 관리 및 보존	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
SI-12	정보 관리 및 보존	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 관리 및 보존	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안 테이블의 연속 백업이 유지됩니다.
SI-12	정보 관리 및 보존	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 관리 및 보존	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-12	정보 관리 및 보존	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-12	정보 관리 및 보존	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	s3-version-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-13(5)	예측 가능한 장애 예방 | 장애 조치 기능	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-20	테인트	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
SI-20	테인트	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
SI-20	테인트	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

템플릿

템플릿은 GitHub: NIST 800-53 rev 5 운영 모범 사례에서 확인할 수 있습니다.

NIST 800 171 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 NIST 800-171과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 NIST 800-171 제어와 관련이 있습니다. NIST 800-171 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에

제어 ID	제어 설명	AWS 구성 규칙	지침
	용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.		IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.1	시스템 액세스를 승인된 사용자, 승인된 사용자를 대신하여 작동하는 프로세스 및 장치(다른 시스템 포함)로 제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.2	시스템 액세스를 승인된 사용자가 실행할 수 있는 유형의 트랜잭션 및 기능으로만 제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3	승인된 권한에 따라 CUI의 흐름을 제어합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.4	개인들의 업무를 분리하여 공모 없이 악의적인 행위의 위험을 줄입니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.5	특정 보안 기능 및 권한 있는 계정 등에 최소 권한의 원칙을 적용합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
3.1.6	비보안 기능에 액세스할 때는 권한이 없는 계정이나 역할을 사용합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.7	권한이 없는 사용자가 권한이 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.7	권한이 없는 사용자가 권한이 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.7	권한이 없는 사용자가 권한이 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
3.1.7	권한이 없는 사용자가 권한이 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.7	권한이 없는 사용자가 권한이 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
3.1.7	권한이 없는 사용자가 권한이 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.7	권한이 없는 사용자가 권한이 있는 기능을 실행하지 못하도록 하고, 해당 기능의 실행을 감사합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.12	원격 액세스 세션을 모니터링하고 제어합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.13	암호화 메커니즘을 사용하여 원격 액세스 세션의 기밀을 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.14	관리형 액세스 제어 지점에서 원격 액세스를 라우팅합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
3.1.20	외부 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.20	외부 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
3.1.20	외부 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.20	외부 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.20	외부 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.20	외부 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.20	외부 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.20	외부 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
3.1.20	외부 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.20	외부 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.20	외부 시스템과의 연결 및 사용을 확인 및 제어/제한합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
3.3.1	불법적이거나 승인되지 않았거나 부적절한 시스템 활동을 모니터링, 분석, 조사 및 보고하는 데 필요한 범위까지 시스템 감사 기록을 생성하고 보관합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.2	개별 시스템 사용자의 작업을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 작업에 대해 책임질 수 있도록 합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.2	개별 시스템 사용자의 작업을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 작업에 대해 책임질 수 있도록 합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
3.3.2	개별 시스템 사용자의 작업을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 작업에 대해 책임질 수 있도록 합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
3.3.2	개별 시스템 사용자의 작업을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 작업에 대해 책임질 수 있도록 합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.2	개별 시스템 사용자의 작업을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 작업에 대해 책임질 수 있도록 합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
3.3.2	개별 시스템 사용자의 작업을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 작업에 대해 책임질 수 있도록 합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.2	개별 시스템 사용자의 작업을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 작업에 대해 책임질 수 있도록 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.2	개별 시스템 사용자의 작업을 해당 사용자에게만 고유하게 추적하여 해당 사용자가 자신의 작업에 대해 책임질 수 있도록 합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.4	감사 프로세스 실패 시 알립니다.	securityhub-enabled	AWS Security Hub 는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.4	감사 프로세스 실패 시 알립니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.5	감사 기록 검토, 분석 및 보고 프로세스를 상호 연계하여 부적절하거나 의심스럽거나 특이한 활동의 징후를 조사하고 이에 대응합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.5	감사 기록 검토, 분석 및 보고 프로세스를 상호 연계하여 부적절하거나 의심스럽거나 특이한 활동의 징후를 조사하고 이에 대응합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
3.3.8	감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.8	감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.8	감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.8	감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.8	감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
3.3.8	감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.8	감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.3.8	감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.8	감사 정보 및 감사 도구를 무단 액세스, 수정 및 삭제로부터 보호합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
3.4.1	각 시스템 개발 주기 전반에 걸쳐 조직 시스템(하드웨어, 소프트웨어, 펌웨어, 문서 포함)의 기본 구성 및 인벤토리를 수립하고 유지합니다.	ec2-security-group-attached-to-eni-periodic	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.1	각 시스템 개발 주기 전반에 걸쳐 조직 시스템(하드웨어, 소프트웨어, 펌웨어, 문서 포함)의 기본 구성 및 인벤토리를 수립하고 유지합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.1	각 시스템 개발 주기 전반에 걸쳐 조직 시스템(하드웨어, 소프트웨어, 펌웨어, 문서 포함)의 기본 구성 및 인벤토리를 수립하고 유지합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
3.4.1	각 시스템 개발 주기 전반에 걸쳐 조직 시스템(하드웨어, 소프트웨어, 펌웨어, 문서 포함)의 기본 구성 및 인벤토리를 수립하고 유지합니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.1	각 시스템 개발 주기 전반에 걸쳐 조직 시스템(하드웨어, 소프트웨어, 펌웨어, 문서 포함)의 기본 구성 및 인벤토리를 수립하고 유지합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
3.4.1	각 시스템 개발 주기 전반에 걸쳐 조직 시스템(하드웨어, 소프트웨어, 펌웨어, 문서 포함)의 기본 구성 및 인벤토리를 수립하고 유지합니다.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.6	필수 기능만 제공하도록 조직 시스템을 구성하여 최소 기능 원칙을 적용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.4.7	불필요한 기능, 포트, 프로토콜 또는 서비스의 사용을 제한, 비활성화 및 금지합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.7	불필요한 기능, 포트, 프로토콜 또는 서비스의 사용을 제한, 비활성화 및 금지합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.7	불필요한 기능, 포트, 프로토콜 또는 서비스의 사용을 제한, 비활성화 및 금지합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.7	불필요한 기능, 포트, 프로토콜 또는 서비스의 사용을 제한, 비활성화 및 금지합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.9	사용자가 설치한 소프트웨어를 제어 및 모니터링합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.9	사용자가 설치한 소프트웨어를 제어 및 모니터링합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
3.5.2	조직 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 장치의 ID를 인증(또는 확인) 합니다.	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.2	조직 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 장치의 ID를 인증(또는 확인) 합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
3.5.2	조직 시스템에 대한 액세스를 허용하기 위한 전제 조건으로 해당 사용자, 프로세스 또는 장치의 ID를 인증(또는 확인) 합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.3	권한 있는 계정에 대한 로컬 및 네트워크 액세스와 권한 없는 계정에 대한 네트워크 액세스에 대해서는 다중 인증을 사용합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
3.5.3	권한 있는 계정에 대한 로컬 및 네트워크 액세스와 권한 없는 계정에 대한 네트워크 액세스에 대해서는 다중 인증을 사용합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.3	권한 있는 계정에 대한 로컬 및 네트워크 액세스와 권한 없는 계정에 대한 네트워크 액세스에 대해서는 다중 인증을 사용합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
3.5.3	권한 있는 계정에 대한 로컬 및 네트워크 액세스와 권한 없는 계정에 대한 네트워크 액세스에 대해서는 다중 인증을 사용합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.5	지정된 기간 동안 식별자의 재사용을 방지합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
3.5.6	지정된 기간 동안 활동이 없으면 식별자를 비활성화합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.7	새 암호를 만들 때 암호 복잡성과 문자 변경을 최소화합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.8	지정된 세대 수에 대한 암호 재사용을 금지합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
3.5.10	암호로 보호된 암호만 저장하고 전송합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1	준비, 탐지, 분석, 격리, 복구 및 사용자 대응 활동을 포함하는 조직 시스템의 운영 인시던트 처리 역량을 구축합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1	준비, 탐지, 분석, 격리, 복구 및 사용자 대응 활동을 포함하는 조직 시스템의 운영 인시던트 처리 역량을 구축합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1	준비, 탐지, 분석, 격리, 복구 및 사용자 대응 활동을 포함하는 조직 시스템의 운영 인시던트 처리 역량을 구축합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1	준비, 탐지, 분석, 격리, 복구 및 사용자 대응 활동을 포함하는 조직 시스템의 운영 인시던트 처리 역량을 구축합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11.2	조직 시스템 및 애플리케이션의 취약성을 정기적으로 검사하고 해당 시스템 및 애플리케이션에 영향을 미치는 새로운 취약성이 확인되면 검사합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11.2	조직 시스템 및 애플리케이션의 취약성을 정기적으로 검사하고 시스템에 영향을 미치는 새로운 취약성이 확인되면 검사합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
3.11.3	위험 평가에 따라 취약성을 개선합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
3.13.1	조직 시스템의 외부 경계 및 주요 내부 경계에서 통신(즉, 조직 시스템에서 전송 또는 수신되는 정보)를 모니터링, 제어 및 보호합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail의 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우, 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.2	조직 시스템 내에 효과적인 정보 보안을 촉진하는 아키텍처 설계, 소프트웨어 개발 기법 및 시스템 엔지니어링 원칙을 적용합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.6	기본적으로 네트워크 통신 트래픽을 거부하고 예외적으로 네트워크 통신 트래픽을 허용합니다(즉, 모두 거부, 예외에 의한 허용).	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.6	기본적으로 네트워크 통신 트래픽을 거부하고 예외적으로 네트워크 통신 트래픽을 허용합니다(즉, 모두 거부, 예외에 의한 허용).	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.6	기본적으로 네트워크 통신 트래픽을 거부하고 예외적으로 네트워크 통신 트래픽을 허용합니다(즉, 모두 거부, 예외에 의한 허용).	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.
3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.8	별도의 물리적 보호 조치로 달리 보호되지 않는 한, 전송 중에 CUI가 무단으로 공개되지 않도록 암호화 메커니즘을 구현하세요.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.13.10	조직 시스템에 사용되는 암호화를 위한 암호화 키를 설정하고 관리합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
3.13.10	조직 시스템에 사용되는 암호화를 위한 암호화 키를 설정하고 관리합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.16	저장 중 CUI의 기밀을 보호합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
3.13.16	저장 중 CUI의 기밀을 보호합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.16	저장 중 CUI의 기밀을 보호합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.13.16	저장 중 CUI의 기밀을 보호합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.16	저장 중 CUI의 기밀을 보호합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.13.16	저장 중 CUI의 기밀을 보호합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.16	저장 중 CUI의 기밀을 보호합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
3.13.16	저장 중 CUI의 기밀을 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
3.13.16	저장 중 CUI의 기밀을 보호합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
3.13.16	저장 중 CUI의 기밀을 보호합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.16	저장 중 CUI의 기밀을 보호합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
3.13.16	저장 중 CUI의 기밀을 보호합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
3.13.16	저장 중 CUI의 기밀을 보호합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.16	저장 중 CUI의 기밀을 보호합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
3.13.16	저장 중 CUI의 기밀을 보호합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.16	저장 중 CUI의 기밀을 보호합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.16	저장 중 CUI의 기밀을 보호합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
3.13.16	저장 중 CUI의 기밀을 보호합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.1	정보 및 시스템 결함을 적시에 식별, 보고 및 수정합니다.	securityhub-enabled	AWS Security Hub 는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.1	정보 및 시스템 결함을 적시에 식별, 보고 및 수정합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.2	조직 시스템 내 적절한 위치에서 악성 코드로부터 보호합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.2	조직 시스템 내 적절한 위치에서 악성 코드로부터 보호합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.3	시스템 보안 경고 및 권고를 모니터링하고 이에 대한 조치를 취합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.4	새 릴리스가 출시되면 악성 코드 보호 메커니즘을 업데이트합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
3.14.6	인바운드 및 아웃바운드 통신 트래픽을 포함한 조직 시스템을 모니터링하여 공격과 잠재적 공격의 징후를 탐지합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.7	조직 시스템의 무단 사용을 식별합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.7	조직 시스템의 무단 사용을 식별합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.7	조직 시스템의 무단 사용을 식별합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
3.14.7	조직 시스템의 무단 사용을 식별합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.7	조직 시스템의 무단 사용을 식별합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
3.14.7	조직 시스템의 무단 사용을 식별합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.7	조직 시스템의 무단 사용을 식별합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
3.14.7	조직 시스템의 무단 사용을 식별합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.7	조직 시스템의 무단 사용을 식별합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
3.14.7	조직 시스템의 무단 사용을 식별합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.7	조직 시스템의 무단 사용을 식별합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.7	조직 시스템의 무단 사용을 식별합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.7	조직 시스템의 무단 사용을 식별합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
3.14.7	조직 시스템의 무단 사용을 식별합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

템플릿

템플릿은 GitHub: NIST 800 171 운영 모범 사례에서 확인할 수 있습니다.

NIST 800 172 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 NIST 800-172와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 NIST 800-172 제어와 관련이 있습니다. NIST 800-172 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를

제어 ID	제어 설명	AWS 구성 규칙	지침
			활성화하여 해당 데이터를 보호합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	alb-desync-mode-check	HTTP 비동기 취약성으로부터 애플리케이션을 보호하려면 애플리케이션 로드 밸런서에서 HTTP 비동기화 완화 모드를 활성화해야 합니다. HTTP 비동기화 문제로 인해 요청 밀수가 발생하고 애플리케이션이 요청 대기열 또는 캐시 중독에 취약해질 수 있습니다. 비동기화 완화 모드에는 모니터링, 방어 및 가장 엄격 모드가 있습니다. 기본 모드는 방어 모드입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	clb-desync-mode-check	HTTP 비동기 취약성으로부터 애플리케이션을 보호하려면 애플리케이션 로드 밸런서에서 HTTP 비동기화 완화 모드를 활성화해야 합니다. HTTP 비동기화 문제로 인해 요청 밀수가 발생하고 애플리케이션이 요청 대기열 또는 캐시 중독에 취약해질 수 있습니다. 비동기화 완화 모드에는 모니터링, 방어 및 가장 엄격 모드가 있습니다. 기본 모드는 방어 모드입니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[과제: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	ec2-token-hop-limit-check	인스턴스 메타데이터 서비스(IMDS) HTTP PUT 응답이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스로 제한되는지 확인합니다. IMDSv2를 사용하면 메타데이터 응답 홉 제한이 1(Config 기본값)로 설정되어 있기 때문에 기본적으로 비밀 토큰이 포함된 PUT 응답은 인스턴스 외부로 이동할 수 없습니다. 이 값이 1보다 크면 토큰은 EC2 인스턴스에서 나갈 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1.3e	[할당: 조직이 정의한 보안 정보 전송 솔루션]을 사용하여 연결된 시스템의 보안 도메인 간 정보 흐름을 제어합니다.	nacl-no-unrestricted-ssh-rdp	포트 22(SSH) 및 포트 3389(RDP)와 같은 네트워크 액세스 제어 목록(NACL)의 원격 서버 관리 포트에 대한 엑세스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 VPC 내 리소스에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
3.2.1e	사회 공학, 지능형 지속적 위협 행위자, 침해 및 의심스러운 행동의 위협을 인식하고 이에 대응하는 데 초점을 맞춘 인식 교육을 [할당: 조직 정의 빈도]에 따라 제공하고, 교육을 [할당: 조직에서 정의한 빈도]로 업데이트하거나 위협에 중대한 변화가 있을 경우 업데이트합니다.	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.2e	자동화된 메커니즘을 사용하여 잘못 구성되거나 승인되지 않은 시스템 구성 요소를 탐지하고, 탐지 후에는 [선택(하나 이상): 구성 요소 제거, 격리 또는 교정 네트워크에 구성 요소 배치]를 수행하여 패치 적용, 재구성 또는 기타 완화 조치를 용이하게 합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
3.4.2e	자동화된 메커니즘을 사용하여 잘못 구성되거나 승인되지 않은 시스템 구성 요소를 탐지하고, 탐지 후에는 [선택(하나 이상): 구성 요소 제거, 격리 또는 교정 네트워크에 구성 요소 배치]를 수행하여 패치 적용, 재구성 또는 기타 완화 조치를 용이하게 합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.2e	자동화된 메커니즘을 사용하여 잘못 구성되거나 승인되지 않은 시스템 구성 요소를 탐지하고, 탐지 후에는 [선택(하나 이상): 구성 요소 제거, 격리 또는 교정 네트워크에 구성 요소 배치]를 수행하여 패치 적용, 재구성 또는 기타 완화 조치를 용이하게 합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.2e	자동화된 메커니즘을 사용하여 잘못 구성되거나 승인되지 않은 시스템 구성 요소를 탐지하고, 탐지 후에는 [선택(하나 이상): 구성 요소 제거, 격리 또는 교정 네트워크에 구성 요소 배치]를 수행하여 패치 적용, 재구성 또는 기타 완화 조치를 용이하게 합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
3.4.3e	자동화된 검색 및 관리 도구를 사용하여 시스템 구성 요소의 인벤토리를 완전하고 정확하며 즉시 사용할 수 있는 최신 상태로 유지합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.3e	자동화된 검색 및 관리 도구를 사용하여 시스템 구성 요소의 인벤토리를 완전하고 정확하며 즉시 사용할 수 있는 최신 상태로 유지합니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
3.4.3e	자동화된 검색 및 관리 도구를 사용하여 시스템 구성 요소의 인벤토리를 완전하고 정확하며 즉시 사용할 수 있는 최신 상태로 유지합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4.3e	자동화된 검색 및 관리 도구를 사용하여 시스템 구성 요소의 인벤토리를 완전하고 정확하며 즉시 사용할 수 있는 최신 상태로 유지합니다.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
3.4.3e	자동화된 검색 및 관리 도구를 사용하여 시스템 구성 요소의 인벤토리를 완전하고 정확하며 즉시 사용할 수 있는 최신 상태로 유지합니다.	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.2e	다중 인증이나 복잡한 계정 관리를 지원하지 않는 시스템 및 시스템 구성 요소의 암호 생성, 보호, 교체 및 관리를 위한 자동화된 메커니즘을 사용합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
3.5.2e	다중 인증이나 복잡한 계정 관리를 지원하지 않는 시스템 및 시스템 구성 요소의 암호 생성, 보호, 교체 및 관리를 위한 자동화된 메커니즘을 사용합니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
3.5.2e	다중 인증이나 복잡한 계정 관리를 지원하지 않는 시스템 및 시스템 구성 요소의 암호 생성, 보호, 교체 및 관리를 위한 자동화된 메커니즘을 사용합니다.	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.2e	다중 인증이나 복잡한 계정 관리를 지원하지 않는 시스템 및 시스템 구성 요소의 암호 생성, 보호, 교체 및 관리를 위한 자동화된 메커니즘을 사용합니다.	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
3.11.1e	[할당: 조직이 정의한 위협 인텔리전스 소스]를 위험 평가의 일환으로 활용하여 조직 시스템, 보안 아키텍처, 보안 솔루션 선택, 모니터링, 위협 추적, 대응 및 복구 활동의 개발을 안내하고 정보를 제공합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.11.2e	사이버 위협 추적 활동 [선택(하나 이상): [할당: 조직 정의 빈도], [할당: 조직 정의 이벤트]]을 수행하여 [할당: 조직 정의 시스템]에서 침해 지표를 검색하고 기존 제어를 우회하는 위협을 탐지, 추적 및 중단합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
3.11.5e	현재 및 축적된 위협 인텔리전스를 기반으로 조직 시스템 및 조직에 대한 예상 위험을 해결하기 위한 보안 솔루션의 효과를 [할당: 조직 정의 빈도]로 평가합니다.	annual-risk-assessment-performed(프로세스 확인)	조직에 대한 연간 위험 평가를 수행합니다. 위험 평가는 식별된 위험 및/또는 취약성이 조직에 영향을 미칠 가능성과 영향을 파악하는 데 도움이 될 수 있습니다.
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.13.4e	[선택(하나 이상): [과제: 조직이 정의한 물리적 격리 기법], [과제: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	nacl-no-unrestricted-ssh-rdp	포트 22(SSH) 및 포트 3389(RDP)와 같은 네트워크 액세스 제어 목록(NACL)의 원격 서버 관리 포트에 대한 엑세스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 VPC 내 리소스에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
3.13.4e	[선택(하나 이상): [할당: 조직이 정의한 물리적 격리 기법], [할당: 조직이 정의한 논리적 격리 기법]]을 조직 시스템 및 시스템 구성 요소에 적용합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.1e	신뢰 메커니즘의 루트 또는 암호화 서명을 사용하여 [할당: 조직이 정의한 중요한 보안 또는 필수 소프트웨어]의 무결성을 확인합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.2e	조직 시스템 및 시스템 구성 요소를 지속적으로 모니터링하여 변칙적이거나 의심스러운 동작이 있는지 확인합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
3.14.2e	조직 시스템 및 시스템 구성 요소를 지속적으로 모니터링하여 변칙적이거나 의심스러운 동작이 있는지 확인합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.2e	조직 시스템 및 시스템 구성 요소를 지속적으로 모니터링하여 변칙적이거나 의심스러운 동작이 있는지 확인합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
3.14.2e	조직 시스템 및 시스템 구성 요소를 지속적으로 모니터링하여 변칙적이거나 의심스러운 동작이 있는지 확인합니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.2e	조직 시스템 및 시스템 구성 요소를 지속적으로 모니터링하여 변칙적이거나 의심스러운 동작이 있는지 확인합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.2e	조직 시스템 및 시스템 구성 요소를 지속적으로 모니터링하여 변칙적이거나 의심스러운 동작이 있는지 확인합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.2e	조직 시스템 및 시스템 구성 요소를 지속적으로 모니터링하여 변칙적이거나 의심스러운 동작이 있는지 확인합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.6e	[할당: 조직이 정의한 외부 조직]에서 얻은 위협 지표 정보와 효과적인 방어 수단을 사용하여 침입 탐지 및 위협 추적을 안내하고 정보를 제공합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
3.14.7e	[할당: 조직이 정의한 검증 방법 또는 기법]을 사용하여 [할당: 조직에서 정의한 보안의 중요하거나 필수적인 소프트웨어, 펌웨어 및 하드웨어 구성 요소]의 정확성을 확인합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.7e	[할당: 조직이 정의한 검증 방법 또는 기법]을 사용하여 [할당: 조직에서 정의한 보안의 중요하거나 필수적인 소프트웨어, 펌웨어 및 하드웨어 구성 요소]의 정확성을 확인합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
3.14.7e	[할당: 조직이 정의한 검증 방법 또는 기법]을 사용하여 [할당: 조직에서 정의한 보안의 중요하거나 필수적인 소프트웨어, 펌웨어 및 하드웨어 구성 요소]의 정확성을 확인합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.14.7e	[할당: 조직이 정의한 검증 방법 또는 기법]을 사용하여 [할당: 조직에서 정의한 보안의 중요하거나 필수적인 소프트웨어, 펌웨어 및 하드웨어 구성 요소]의 정확성을 확인합니다.	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. AWS Fargate 플랫폼 버전에 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.
3.14.7e	[할당: 조직이 정의한 검증 방법 또는 기법]을 사용하여 [할당: 조직에서 정의한 보안의 중요하거나 필수적인 소프트웨어, 펌웨어 및 하드웨어 구성 요소]의 정확성을 확인합니다.	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository(ECR) 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.

템플릿

템플릿은 GitHub: NIST 800 172 운영 모범 사례에서 확인할 수 있습니다.

NIST 800 181 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 NIST 800 181과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 NIST 800 181 제어와 관련이 있습니다. NIST 800 181 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션

제어 ID	제어 설명	AWS 구성 규칙	지침
			을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0008	데이터 용량 요구 사항의 예상 변화를 분석하고 계획합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암 호화 기간이 종료되면 키가 교체되도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elasticsearch Service(Amazon ES) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0017	서비스 지향 보안 아키텍처 원칙을 적용하여 조직의 기밀성, 무결성 및 가용성 요구 사항을 충족시킵니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
T0024	시스템 사이버 보안 보고를 충족하는 데 필요한 데이터를 수집하고 유지합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0042	사이버 방어 분석가와 협력하여 특수 사이버 방어 애플리케이션을 위한 규칙 및 서명(예: 침입 탐지 및 보호 시스템, 안티바이러스, 콘텐츠 블랙리스트) 업데이트를 관리하고 운영합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
T0047	인시던트 데이터를 상호 연관시켜 특정 취약성을 식별하고 신속한 해결이 가능한 권장 사항을 제시합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 하세요.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0051	크리티컬 시스템 기능을 기반으로 적절한 수준의 시스템 가용성을 정의하고 시스템 요구 사항이 적절한 재해 복구 및 운영 연속성 요구 사항을 식별하여 적절한 장애 조치/대체 사이트 요구 사항, 백업 요구 사항 및 시스템 복구/복원을 위한 물질적 지원 요구 사항을 포함하도록 합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
T0065	네트워크 백업 및 복구 절차를 개발하고 구현합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장하세요.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0070	개발 중인 시스템에 대한 재해 복구 및 운영 연속성 계획을 수립하고 시스템이 프로덕션 환경에 들어가기 전에 테스트하는 것을 보장합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0086	시스템 설계에 통합된 상용 제품의 보안 패치 적용이 의도한 운영 환경에 대해 관리 기관이 지정한 타임라인을 준수하는지 확인합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
T0086	시스템 설계에 통합된 상용 제품의 보안 패치 적용이 의도한 운영 환경에 대해 관리 기관이 지정한 타임라인을 준수하는지 확인하세요.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0086	시스템 설계에 통합된 상용 제품의 보안 패치 적용이 의도한 운영 환경에 대해 관리 기관이 지정한 타임라인을 준수하는지 확인합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0086	시스템 설계에 통합된 상용 제품의 보안 패치 적용이 의도한 운영 환경에 대해 관리 기관이 지정한 타임라인을 준수하는지 확인합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0110	보안 인시던트가 특정 법적 조치가 필요한 법률 위반인지 여부를 식별 및/또는 판단합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0110	보안 인시던트가 특정 법적 조치가 필요한 법률 위반인지 여부를 식별 및/또는 판단합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0110	보안 인시던트가 특정 법적 조치가 필요한 법률 위반인지 여부를 식별 및/또는 판단합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
T0128	가능한 경우 시스템 소프트웨어 업데이트 또는 패치 적용을 위한 자동화 기능을 포함하고 시스템 운영 환경에 대한 현재 및 예상 패치 타임라인 요구 사항을 기반으로 시스템 소프트웨어의 수동 업데이트 및 패치 적용을 위한 프로세스와 절차를 개발합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0128	가능한 경우 시스템 소프트웨어 업데이트 또는 패치 적용을 위한 자동화 기능을 포함하고 시스템 운영 환경에 대한 현재 및 예상 패치 타임라인 요구 사항을 기반으로 시스템 소프트웨어의 수동 업데이트 및 패치 적용을 위한 프로세스와 절차를 개발합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
T0128	가능한 경우 시스템 소프트웨어 업데이트 또는 패치 적용을 위한 자동화 기능을 포함하고 시스템 운영 환경에 대한 현재 및 예상 패치 타임라인 요구 사항을 기반으로 시스템 소프트웨어의 수동 업데이트 및 패치 적용을 위한 프로세스와 절차를 개발합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0128	가능한 경우 시스템 소프트웨어 업데이트 또는 패치 적용을 위한 자동화 기능을 포함하고 시스템 운영 환경에 대한 현재 및 예상 패치 타임라인 요구 사항을 기반으로 시스템 소프트웨어의 수동 업데이트 및 패치 적용을 위한 프로세스와 절차를 개발합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	opensearch-in-vpc-only	Amazon Elasticsearch Service(Amazon ES) 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon ES 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon ES와 다른 서비스 간에 보안 통신이 가능합니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
T0144	계정, 네트워크 권한, 시스템 및 장비에 대한 액세스를 관리합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0151	사이버 보안 보호 장치가 의도한 수준의 보호를 제공하는지 모니터링하고 그 효과를 평가하세요.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0151	사이버 보안 보호 장치가 의도한 수준의 보호를 제공하는지 모니터링하고 그 효과를 평가하세요.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0151	사이버 보안 보호 장치가 의도한 수준의 보호를 제공하는지 모니터링하고 그 효과를 평가하세요.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지관리합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지관리합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지관리합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지관리합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지관리합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0152	최적의 성능을 보장하기 위해 데이터베이스를 모니터링하고 유지 관리합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0153	네트워크 용량 및 성능을 모니터링합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0153	네트워크 용량 및 성능을 모니터링합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0153	네트워크 용량 및 성능을 모니터링합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0153	네트워크 용량 및 성능을 모니터링합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 강화된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
T0154	지식 관리 자산 및 자원의 사용을 모니터링하고 보고합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0156	구성 관리를 감독하고 관련 권장 사항을 제시합니다.	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
T0156	구성 관리를 감독하고 관련 권장 사항을 제시합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0156	구성 관리를 감독하고 관련 권장 사항을 제시합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
T0156	구성 관리를 감독하고 관련 권장 사항을 제시합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0156	구성 관리를 감독하고 관련 권장 사항을 제시합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0156	구성 관리를 감독하고 관련 권장 사항을 제시합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
T0156	구성 관리를 감독하고 관련 권장 사항을 제시합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0156	구성 관리를 감독하고 관련 권장 사항을 제시합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0156	구성 관리를 감독하고 관련 권장 사항을 제시합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
T0160	네트워크 취약성을 패치하여 외부자로부터 정보가 보호되도록 합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0160	네트워크 취약성을 패치하여 외부자로부터 정보가 보호되도록 합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
T0160	네트워크 취약성을 패치하여 외부자로부터 정보가 보호되도록 합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도 및 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
T0162	데이터베이스의 백업 및 복구를 수행하여 데이터 무결성을 보장합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
T0166	기업 내에서 다양한 출처에서 수집한 정보를 바탕으로 이벤트 상관관계를 분석하여 상황을 파악하고 관찰된 공격의 유효성을 판단합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0168	설정된 데이터베이스와 해시 비교를 수행합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	opensearch-in-vpc-only	Amazon Elasticsearch Service(Amazon ES) 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon ES 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon ES와 다른 서비스 간에 보안 통신이 가능합니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0195	임무 요구 사항에 따라 관련 정보의 관리 흐름을 제공(웹 기반 포털 또는 기타 수단을 통해)합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
T0215	보안 위반 가능성을 인지하고 필요에 따라 적절한 조치를 취하여 인시던트를 보고합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0244	애플리케이션 소프트웨어, 네트워크, 및 시스템의 보안 조치가 명시된 대로 구현되었는지 확인하고, 편차를 문서화하고, 이러한 편차를 수정하는 데 필요한 조치를 권장합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0244	애플리케이션 소프트웨어, 네트워크, 및 시스템의 보안 조치가 명시된 대로 구현되었는지 확인하고, 편차를 문서화하고, 이러한 편차를 수정하는 데 필요한 조치를 권장합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0244	애플리케이션 소프트웨어, 네트워크, 및 시스템의 보안 조치가 명시된 대로 구현되었는지 확인하고, 편차를 문서화하고, 이러한 편차를 수정하는 데 필요한 조치를 권장합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
T0258	가능한 공격/침입, 변칙 활동 및 악용 활동을 적시에 탐지, 식별 및 경고하고 이러한 인시던트 및 이벤트를 무해한 활동과 구별합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0259	사이버 방어 도구를 사용하여 시스템 활동을 지속적으로 모니터링하고 분석하여 악의적인 활동을 식별합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	opensearch-in-vpc-only	Amazon Elasticsearch Service(Amazon ES) 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon ES 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon ES와 다른 서비스 간에 보안 통신이 가능합니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0262	승인된 심층 방어 원칙 및 사례(예: 다중 장소에서의 방어, 계층적 방어, 보안 견고성)를 이용합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-policy-no-stat ements-with-full-a ccess	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 보안 인증 정보가 포함되지 않도록 합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	opensearch-in-vpc-only	Amazon Elasticsearch Service(Amazon ES) 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon ES 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon ES와 다른 서비스 간에 보안 통신이 가능합니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0284	사이버 보안과 관련된 새로운 도구 및 기술을 설계하고 개발합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0306	데이터베이스 및 데이터 관리 시스템에 대한 인시던트 관리, 서비스 수준 관리, 변경 관리, 릴리스 관리, 연속성 관리, 가용성 관리를 지원합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0306	데이터베이스 및 데이터 관리 시스템에 대한 인시던트 관리, 서비스 수준 관리, 변경 관리, 릴리스 관리, 연속성 관리, 가용성 관리를 지원합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0306	데이터베이스 및 데이터 관리 시스템에 대한 인시던트 관리, 서비스 수준 관리, 변경 관리, 릴리스 관리, 연속성 관리, 가용성 관리를 지원합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
T0314	시스템 보안 컨텍스트인 예비 시스템 보안 운영 개념(CONOPS)을 개발하고 해당 사이버 보안 요구 사항에 따라 기본 시스템 보안 요구 사항을 정의합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0314	시스템 보안 컨텍스트인 예비 시스템 보안 운영 개념(CONOPS)을 개발하고 해당 사이버 보안 요구 사항에 따라 기본 시스템 보안 요구 사항을 정의합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
T0314	시스템 보안 컨텍스트인 예비 시스템 보안 운영 개념(CONOPS)을 개발하고 해당 사이버 보안 요구 사항에 따라 기본 시스템 보안 요구 사항을 정의합니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0314	시스템 보안 컨텍스트인 예비 시스템 보안 운영 개념(CONOPS)을 개발하고 해당 사이버 보안 요구 사항에 따라 기본 시스템 보안 요구 사항을 정의합니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
T0314	시스템 보안 컨텍스트인 예비 시스템 보안 운영 개념(CONOPS)을 개발하고 해당 사이버 보안 요구 사항에 따라 기본 시스템 보안 요구 사항을 정의합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0314	시스템 보안 컨텍스트인 예비 시스템 보안 운영 개념(CONOPS)을 개발하고 해당 사이버 보안 요구 사항에 따라 기본 시스템 보안 요구 사항을 정의합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0333	사이버 방어 추세를 분석하고 보고합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0333	사이버 방어 추세를 분석하고 보고합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
T0347	소스 데이터 및 후속 조사 결과의 타당성을 평가합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0358	권한 있는 액세스 사용자를 위한 시스템 관리 및 관리 기능을 설계하고 개발합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
T0358	권한 있는 액세스 사용자를 위한 시스템 관리 및 관리 기능을 설계하고 개발합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0358	권한 있는 액세스 사용자를 위한 시스템 관리 및 관리 기능을 설계하고 개발합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0358	권한 있는 액세스 사용자를 위한 시스템 관리 및 관리 기능을 설계하고 개발합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0358	권한 있는 액세스 사용자를 위한 시스템 관리 및 관리 기능을 설계하고 개발합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0358	권한 있는 액세스 사용자를 위한 시스템 관리 및 관리 기능을 설계하고 개발합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0358	권한 있는 액세스 사용자를 위한 시스템 관리 및 관리 기능을 설계하고 개발합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0358	권한 있는 액세스 사용자를 위한 시스템 관리 및 관리 기능을 설계하고 개발합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0376	조직 요구 사항에 따라 사이버 인력 관리 프로그램을 수립, 자원 조달, 구현 및 평가합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
T0416	기존 공개 키 인프라(PKI) 라이브러리를 활용하고 적절한 경우 인증서 관리 및 암호화 기능을 통합하여 공개 키로 애플리케이션을 활성화합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0416	기존 공개 키 인프라(PKI) 라이브러리를 활용하고 적절한 경우 인증서 관리 및 암호화 기능을 통합하여 공개 키로 애플리케이션을 활성화합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0416	기존 공개 키 인프라(PKI) 라이브러리를 활용하고 적절한 경우 인증서 관리 및 암호화 기능을 통합하여 공개 키로 애플리케이션을 활성화합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0416	기존 공개 키 인프라 (PKI) 라이브러리를 활용하고 적절한 경우 인증서 관리 및 암호화 기능을 통합하여 공개 키로 애플리케이션을 활성화합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
T0416	기존 공개 키 인프라 (PKI) 라이브러리를 활용하고 적절한 경우 인증서 관리 및 암호화 기능을 통합하여 공개 키로 애플리케이션을 활성화합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0416	기존 공개 키 인프라(PKI) 라이브러리를 활용하고 적절한 경우 인증서 관리 및 암호화 기능을 통합하여 공개 키로 애플리케이션을 활성화합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0416	기존 공개 키 인프라(PKI) 라이브러리를 활용하고 적절한 경우 인증서 관리 및 암호화 기능을 통합하여 공개 키로 애플리케이션을 활성화합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0416	기존 공개 키 인프라(PKI) 라이브러리를 활용하고 적절한 경우 인증서 관리 및 암호화 기능을 통합하여 공개 키로 애플리케이션을 활성화합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0416	기존 공개 키 인프라(PKI) 라이브러리를 활용하고 적절한 경우 인증서 관리 및 암호화 기능을 통합하여 공개 키로 애플리케이션을 활성화합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0416	기존 공개 키 인프라(PKI) 라이브러리를 활용하고 적절한 경우 인증서 관리 및 암호화 기능을 통합하여 공개 키로 애플리케이션을 활성화합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0421	명시적인 조직 지식(예: 하드카피 문서, 디지털 파일)의 인덱싱/카탈로그 작성, 저장 및 액세스를 관리합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	opensearch-in-vpc-only	Amazon Elasticsearch Service(Amazon ES) 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon ES 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon ES와 다른 서비스 간에 보안 통신이 가능합니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
T0475	최소 권한 및 알아야 할 필요성 원칙에 따라 적절한 액세스 제어를 평가합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
T0489	기밀성, 무결성, 가용성, 인증 및 부인 방지를 보장하기 위해 확립된 절차에 따라 시스템 보안 조치를 구현합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0491	조직 표준에 따라 시스템 사용자를 위한 하드웨어, 소프트웨어 및 주변 장치를 설치하고 구성합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0491	조직 표준에 따라 시스템 사용자를 위한 하드웨어, 소프트웨어 및 주변 장치를 설치하고 구성합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
T0491	조직 표준에 따라 시스템 사용자를 위한 하드웨어, 소프트웨어 및 주변 장치를 설치하고 구성합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0503	외부 데이터 소스(예: 사이버 방어 공급업체 사이트, 컴퓨터 비상 대응팀, Security Focus)를 모니터링하여 사이버 방어 위협 상황을 최신으로 유지하고 기업에 영향을 미칠 수 있는 보안 문제를 파악합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
T0509	정보 보안 위험 평가를 수행합니다.	annual-risk-assessment-performed(프로세스 확인)	조직에 대한 연간 위험 평가를 수행합니다. 위험 평가는 식별된 위험 및/또는 취약성이 조직에 영향을 미칠 가능성과 영향을 파악하는 데 도움이 될 수 있습니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	elasticsearch-node-to-node-encryption-check	Amazon Elasticsearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	opensearch-encrypt ed-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elasticsearch Service(Amazon ES) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	opensearch-node-to-node-encryption-check	Amazon Elasticsearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 되므로 Amazon Elasticsearch Service(Amazon ES) 도메인에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0553	사이버 보안 기능(예: 암호화, 액세스 제어, ID 관리)을 적용하여 악용 기회를 낮춥니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
T0557	사이버 공간과 관련된 주요 관리 기능을 통합합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암 호화 기간이 종료되면 키가 교체되도록 합니다.
T0557	사이버 공간과 관련된 주요 관리 기능을 통합합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0576	모든 출처의 인텔리전스를 평가하고 사이버 운영 목표를 지원하는 대상을 추천합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	elasticsearch-in-vpc-only	Amazon Elasticsearch Service(Amazon ES) 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon ES 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon ES와 다른 서비스 간에 보안 통신이 가능합니다.
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	opensearch-in-vpc-only	Amazon Elasticsearch Service(Amazon ES) 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon ES 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon ES와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0609	무선 컴퓨터 및 디지털 네트워크의 액세스를 활성화합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
T0616	네트워크 내 시스템의 네트워크 스카우팅 및 취약성 분석을 수행합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0686	위협 취약성을 식별합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
T0686	위협 취약성을 식별합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	elasticsearch-logs-to-cloudwatch	Amazon Elasticsearch 서비스 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 강화된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
T0706	기존 기법 및 대체 기법(예: 소셜 네트워크 분석, 콜체인, 트래픽 분석)을 통해 네트워크에 대한 정보를 수집합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0777	프로필 네트워크 또는 시스템 관리자 및 해당 활동	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
T0805	인텔리전스에서 파생된 중요한 네트워크 이벤트 및 침입을 보고합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0877	관련 조직 부서와 협력하여 소비자 정보 액세스 권한을 감독합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
T0877	관련 조직 부서와 협력하여 소비자 정보 액세스 권한을 감독합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
T0877	관련 조직 부서와 협력하여 소비자 정보 액세스 권한을 감독합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0877	관련 조직 부서와 협력하여 소비자 정보 액세스 권한을 감독합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0877	관련 조직 부서와 협력하여 소비자 정보 액세스 권한을 감독합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0877	관련 조직 부서와 협력하여 소비자 정보 액세스 권한을 감독합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0877	관련 조직 부서와 협력하여 소비자 정보 액세스 권한을 감독합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
T0877	관련 조직 부서와 협력하여 소비자 정보 액세스 권한을 감독합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0877	관련 조직 부서와 협력하여 소비자 정보 액세스 권한을 감독합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0877	관련 조직 부서와 협력하여 소비자 정보 액세스 권한을 감독합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0877	관련 조직 부서와 협력하여 소비자 정보 액세스 권한을 감독합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
T0935	정보 보안 위험 평가를 수행합니다.	annual-risk-assessment-performed(프로세스 확인)	조직에 대한 연간 위험 평가를 수행합니다. 위험 평가는 식별된 위험 및/또는 취약성이 조직에 영향을 미칠 가능성과 영향을 파악하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0960	시스템 및 시스템 운영 환경의 변화를 모니터링합니다.	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.
T0960	시스템 및 시스템 운영 환경의 변화를 모니터링합니다.	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0960	시스템 및 시스템 운영 환경의 변화를 모니터링합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0960	시스템 및 시스템 운영 환경의 변화를 모니터링합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0960	시스템 및 시스템 운영 환경의 변화를 모니터링합니다.	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 강화된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0960	시스템 및 시스템 운영 환경의 변화를 모니터링합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0960	시스템 및 시스템 운영 환경의 변화를 모니터링합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0960	시스템 및 시스템 운영 환경의 변화를 모니터링합니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0992	지속적 모니터링 결과를 상시 권한 부여에 어떻게 사용할 것인지 결정합니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
T0993	지속적인 모니터링 도구 그리고 기술 액세스 제어 프로세스 및 절차를 수립합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

템플릿

템플릿은 GitHub: NIST 800 181 운영 모범 사례에서 확인할 수 있습니다.

NIST 1800 25 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 NIST 1800-25와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각각은 특정 AWS 리소스에 AWS Config 적용되며 하나 이상의 NIST 1800-25 제어와 관련이 있습니다. NIST 1800-25 제어는 여러 AWS Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.AM-2	조직 내 소프트웨어 플랫폼 및 애플리케이션 인벤토리가 작성됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.AM-2	조직 내 소프트웨어 플랫폼 및 애플리케이션 인벤토리가 작성됩니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
ID.AM-2	조직 내 소프트웨어 플랫폼 및 애플리케이션 인벤토리가 작성됩니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.AM-2	조직 내 소프트웨어 플랫폼 및 애플리케이션 인벤토리가 작성됩니다.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
ID.AM-2	조직 내 소프트웨어 플랫폼 및 애플리케이션 인벤토리가 작성됩니다.	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.RA1	자산 취약성이 식별되고 문서화됩니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
ID.RA1	자산 취약성이 식별되고 문서화됩니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.RA1	자산 취약성이 식별되고 문서화됩니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
ID.RA1	자산 취약성이 식별되고 문서화됩니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
PR.AC-3	원격 액세스가 관리됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
PR.AC-3	원격 액세스가 관리됩니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
PR.AC-3	원격 액세스가 관리됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-3	원격 액세스가 관리됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-3	원격 액세스가 관리됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-3	원격 액세스가 관리됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-3	원격 액세스가 관리됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-3	원격 액세스가 관리됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
PR.AC-3	원격 액세스가 관리됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.AC-3	원격 액세스가 관리됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
PR.AC-3	원격 액세스가 관리됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
PR.DS-1	저장 데이터는 보호됩니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-1	저장 데이터는 보호됩니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-1	저장 데이터는 보호됩니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-1	저장 데이터는 보호됩니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
PR.DS-1	저장 데이터는 보호됩니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
PR.DS-1	저장 데이터는 보호됩니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
PR.DS-1	저장 데이터는 보호됩니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
PR.DS-1	저장 데이터는 보호됩니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-1	저장 데이터는 보호됩니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-1	저장 데이터는 보호됩니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-2	전송 중 데이터는 보호됩니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-2	전송 중 데이터는 보호됩니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-2	전송 중 데이터는 보호됩니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-2	전송 중 데이터는 보호됩니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-2	전송 중 데이터는 보호됩니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-2	전송 중 데이터는 보호됩니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-2	전송 중 데이터는 보호됩니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
PR.DS-2	전송 중 데이터는 보호됩니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-2	전송 중 데이터는 보호됩니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-6	무결성 검사 메커니즘은 소프트웨어, 펌웨어 및 정보 무결성을 확인하는 데 사용됩니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-6	무결성 검사 메커니즘은 소프트웨어, 펌웨어 및 정보 무결성을 확인하는 데 사용됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
PR.IP-3	구성 변경 제어 프로세스가 갖춰져 있습니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-3	구성 변경 제어 프로세스가 갖춰져 있습니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-9	대응 계획 (사고 대응 및 비즈니스 연속성) 및 복구 계획 (사고 복구 및 재해 복구) 이 마련되어 관리됩니다.	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되는지 확인하세요. 대응 계획을 업데이트하고 공식적으로 문서화하면 대응 담당자가 역할, 책임 및 사고 발생 시 따라야 할 프로세스를 이해하는 데 도움이 될 수 있습니다.
PR.IP-10	대응 및 복구 계획을 테스트합니다.	response-plan-tested(프로세스 확인)	사고 대응 및 복구 계획이 테스트되었는지 확인합니다. 이는 인시던트 발생 중에 해당 계획이 효과적인지 그리고 격차나 업데이트를 해결해야 하는지를 이해하는 데 도움이 될 수 있습니다.
PR.IP-12	취약성 관리 계획이 개발되고 구현됩니다.	vuln-management-plan-exists(프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 프로세스를 공식적으로 정의하려면 취약성 관리 계획을 개발하고 구현해야 합니다. 여기에는 취약성 관리 도구, 환경 검사 주기, 역할 및 책임이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-12	취약성 관리 계획이 개발되고 구현됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-12	취약성 관리 계획이 개발되고 구현됩니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
PR.IP-12	취약성 관리 계획이 개발되고 구현됩니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.MA-2	조직 자산의 원격 유지 관리는 무단 액세스를 방지하는 방식으로 승인, 기록 및 수행됩니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.MA-2	조직 자산의 원격 유지 관리는 무단 액세스를 방지하는 방식으로 승인, 기록 및 수행됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	통신 및 제어 네트워크가 보호됩니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
DE.CM-8	취약성 스캔이 수행됩니다.	vuln-scans-performed(프로세스 확인)	규정 준수 요구 사항에 따라 취약성 스캔이 수행되는지 확인합니다. 검사 주기, 사용하는 도구, 결과 사용은 조직에서 정의해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.MI-3	새로 식별된 취약성은 완화되거나 허용되는 위험으로 문서화됩니다.	vuln-mitigated-accepted(프로세스 확인)	새로 식별된 취약성이 교정되거나 허용된 위험으로 문서화되는지 확인합니다. AWS Security Hub, Amazon Guard Duty, Amazon Inspector 및 AWS Config와 같은 서비스는 환경 내의 취약성을 식별하는 데 도움이 될 수 있습니다. 취약성은 조직의 규정 준수 요구 사항에 따라 교정하거나 허용된 위험으로 처리해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.MI-3	새로 식별된 취약성은 완화되거나 허용되는 위험으로 문서화됩니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

템플릿

템플릿은 GitHub: NIST 1800 25 운영 모범 사례에서 확인할 수 있습니다.

NIST CSF 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 NIST 사이버 보안 프레임워크(CSF)와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 AWS Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 NIST CSF 제어와 관련이 있습니다.

NIST CSF 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면

제어 ID	제어 설명	AWS 구성 규칙	지침
			CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-1	사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름의 기준선이 설정되고 관리됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-2	탐지된 이벤트를 분석하여 공격 대상 및 기법을 파악합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
DE.AE-2	탐지된 이벤트를 분석하여 공격 대상 및 기법을 파악합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
DE.AE-3	이벤트 데이터는 여러 소스 및 센서에서 수집되고 상호 연관됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-4	이벤트의 영향이 결정됩니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
DE.AE-4	이벤트의 영향을 판단합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-4	이벤트의 영향을 판단합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
DE.AE-4	이벤트의 영향을 판단합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-4	이벤트의 영향을 판단합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-4	이벤트의 영향을 판단합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-4	이벤트의 영향을 판단합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.AE-4	이벤트의 영향을 판단합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
DE.CM-1	네트워크를 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-1	네트워크를 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
DE.CM-1	네트워크를 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-1	네트워크를 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
DE.CM-1	네트워크를 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-1	네트워크를 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-1	네트워크를 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
DE.CM-1	네트워크를 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	s3-event-notifications-enabled	Amazon S3 이벤트 알림은 버킷 객체가 우발적이거나 의도적으로 수정된 경우 관련 담당자에게 알릴 수 있습니다. 알림의 예로는 새 객체 생성, 객체 제거, 객체 복원, 분실 및 복제된 객체 등이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-1	네트워크를 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-1	네트워크를 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
DE.CM-3	직원 활동을 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-3	직원 활동을 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
DE.CM-3	직원 활동을 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-3	직원 활동을 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-3	직원 활동을 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-3	직원 활동을 모니터링하여 잠재적 사이버 보안 이벤트를 탐지합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-4	악성 코드를 탐지합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
DE.CM-4	악성 코드를 탐지합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-5	승인되지 않은 모바일 코드가 감지됩니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
DE.CM-5	승인되지 않은 모바일 코드가 감지됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-5	승인되지 않은 모바일 코드가 감지됩니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
DE.CM-5	승인되지 않은 모바일 코드가 감지됩니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-5	승인되지 않은 모바일 코드가 감지됩니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-5	승인되지 않은 모바일 코드가 감지됩니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
DE.CM-6	외부 서비스 제공업체 활동을 모니터링하여 잠재적인 사이버 보안 이벤트를 탐지합니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-6	외부 서비스 제공업체 활동을 모니터링하여 잠재적인 사이버 보안 이벤트를 탐지합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
DE.CM-6	외부 서비스 제공업체 활동을 모니터링하여 잠재적인 사이버 보안 이벤트를 탐지합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-6	외부 서비스 제공업체 활동을 모니터링하여 잠재적인 사이버 보안 이벤트를 탐지합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-6	외부 서비스 제공업체 활동을 모니터링하여 잠재적인 사이버 보안 이벤트를 탐지합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-6	외부 서비스 제공업체 활동을 모니터링하여 잠재적인 사이버 보안 이벤트를 탐지합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
DE.CM-7	승인되지 않은 사용자, 연결, 장치 및 소프트웨어에 대한 모니터링을 수행합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-7	승인되지 않은 사용자, 연결, 장치 및 소프트웨어에 대한 모니터링을 수행합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
DE.CM-7	승인되지 않은 사용자, 연결, 장치 및 소프트웨어에 대한 모니터링을 수행합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-7	승인되지 않은 사용자, 연결, 장치 및 소프트웨어에 대한 모니터링을 수행합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
DE.CM-7	승인되지 않은 사용자, 연결, 장치 및 소프트웨어에 대한 모니터링을 수행합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-7	승인되지 않은 사용자, 연결, 장치 및 소프트웨어에 대한 모니터링을 수행합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-7	승인되지 않은 사용자, 연결, 장치 및 소프트웨어에 대한 모니터링을 수행합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-7	승인되지 않은 사용자, 연결, 장치 및 소프트웨어에 대한 모니터링을 수행합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.CM-7	승인되지 않은 사용자, 연결, 장치 및 소프트웨어에 대한 모니터링을 수행합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
DE.DP-4	이벤트 감지 정보를 알립니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.DP-4	이벤트 감지 정보를 알립니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
DE.DP-4	이벤트 감지 정보를 알립니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.DP-4	이벤트 감지 정보를 알립니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
DE.DP-4	이벤트 감지 정보를 알립니다.	s3-event-notifications-enabled	Amazon S3 이벤트 알림은 버킷 객체가 우발적이거나 의도적으로 수정된 경우 관련 담당자에게 알릴 수 있습니다. 알림의 예로는 새 객체 생성, 객체 제거, 객체 복원, 분실 및 복제된 객체 등이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.DP-4	이벤트 감지 정보를 알립니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
DE.DP-4	이벤트 감지 정보를 알립니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
DE.DP-5	탐지 프로세스를 지속적으로 개선합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.AM-2	조직 내 소프트웨어 플랫폼 및 애플리케이션 인벤토리가 작성됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.AM-2	조직 내 소프트웨어 플랫폼 및 애플리케이션 인벤토리가 작성됩니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
ID.AM-2	조직 내 소프트웨어 플랫폼 및 애플리케이션 인벤토리가 작성됩니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.AM-2	조직 내 소프트웨어 플랫폼 및 애플리케이션 인벤토리가 작성됩니다.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
ID.AM-2	조직 내 소프트웨어 플랫폼 및 애플리케이션 인벤토리가 작성됩니다.	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
ID.AM-3	조직 커뮤니케이션 및 데이터 흐름이 매핑됩니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.AM-3	조직 커뮤니케이션 및 데이터 흐름이 매핑됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
ID.AM-3	조직 커뮤니케이션 및 데이터 흐름이 매핑됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.AM-3	조직 커뮤니케이션 및 데이터 흐름이 매핑됩니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.AM-3	조직 커뮤니케이션 및 데이터 흐름이 매핑됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.AM-3	조직 커뮤니케이션 및 데이터 흐름이 매핑됩니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
ID.AM-3	조직 커뮤니케이션 및 데이터 흐름이 매핑됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.BE-5	중요 서비스 제공을 지원하기 위해 필요한 복원력 요구 사항을 모든 운영 상태(예: 압박/공격 상황, 복구 중, 정상 운영)에 대해 설정합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.RA-1	자산 취약성이 식별되고 문서화됩니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.
ID.RA1	자산 취약성이 식별되고 문서화됩니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.RA1	자산 취약성이 식별되고 문서화됩니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
ID.RA1	자산 취약성이 식별되고 문서화됩니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.RA-2	사이버 위협 인텔리전스를 정보 공유 포럼 및 출처에서 수신합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
ID.RA-3	내부 및 외부 위협을 식별하고 문서화합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.RA-3	내부 및 외부 위협을 식별하고 문서화합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
ID.RA-5	위협, 취약성, 가능성 및 영향을 사용하여 위험을 판단합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.RA-5	위협, 취약성, 가능성 및 영향을 사용하여 위험을 판단합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.RA-5	위협, 취약성, 가능성 및 영향을 사용하여 위험을 판단합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.RA-5	위협, 취약성, 가능성 및 영향을 사용하여 위험을 판단합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
ID.SC-4	공급업체 및 타사 파트너가 정기적으로 감사, 테스트 결과 또는 기타 형식의 평가를 통해 계약상 의무를 준수하고 있는지 확인합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.SC-4	공급업체 및 타사 파트너가 정기적으로 감사, 테스트 결과 또는 기타 형식의 평가를 통해 계약상 의무를 준수하고 있는지 확인합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.SC-4	공급업체 및 타사 파트너가 정기적으로 감사, 테스트 결과 또는 기타 형식의 평가를 통해 계약상 의무를 준수하고 있는지 확인합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
ID.SC-4	공급업체 및 타사 파트너가 정기적으로 감사, 테스트 결과 또는 기타 형식의 평가를 통해 계약상 의무를 준수하고 있는지 확인합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-1	승인된 장치, 사용자 및 프로세스에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사됩니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
PR.AC-3	원격 액세스가 관리됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
PR.AC-3	원격 액세스가 관리됩니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
PR.AC-3	원격 액세스가 관리됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-3	원격 액세스가 관리됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-3	원격 액세스가 관리됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-3	원격 액세스가 관리됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-3	원격 액세스가 관리됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-3	원격 액세스가 관리됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.AC-3	원격 액세스가 관리됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.AC-3	원격 액세스가 관리됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-3	원격 액세스가 관리됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.AC-4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-6	ID는 증명되고 보안 인증 정보에 구속되며 상호 작용에서 주장됩니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-6	ID는 증명되고 보안 인증 정보에 구속되며 상호 작용에서 주장됩니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-7	사용자, 장치 및 기타 자산은 거래 위험(예: 개인의 보안 및 개인정보보호 위험 및 기타 조직적 위험)에 상응하는 인증(예: 단일 요소, 다중 요소)을 거칩니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
PR.AC-7	사용자, 장치 및 기타 자산은 거래 위험(예: 개인의 보안 및 개인정보보호 위험 및 기타 조직적 위험)에 상응하는 인증(예: 단일 요소, 다중 요소)을 거칩니다.	iam-user-mfa-enabled	이 규칙을 사용하면 AWS 클라우드의 리소스에 대한 액세스를 제한할 수 있습니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-7	사용자, 장치 및 기타 자산은 거래 위험(예: 개인의 보안 및 개인정보보호 위험 및 기타 조직적 위험)에 상응하는 인증(예: 단일 요소, 다중 요소)을 거칩니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-7	사용자, 장치 및 기타 자산은 거래 위험(예: 개인의 보안 및 개인정보보호 위험 및 기타 조직적 위험)에 상응하는 인증(예: 단일 요소, 다중 요소)을 거칩니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
PR.AC-7	사용자, 장치 및 기타 자산은 거래 위험(예: 개인의 보안 및 개인정보보호 위험 및 기타 조직적 위험)에 상응하는 인증(예: 단일 요소, 다중 요소)을 거칩니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AT-1	모든 사용자에게 정보 및 교육을 제공합니다.	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.
PR.DS-1	저장 데이터는 보호됩니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-1	저장 데이터는 보호됩니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-1	저장 데이터는 보호됩니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-1	저장 데이터는 보호됩니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
PR.DS-1	저장 데이터는 보호됩니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
PR.DS-1	저장 데이터는 보호됩니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
PR.DS-1	저장 데이터는 보호됩니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
PR.DS-1	저장 데이터는 보호됩니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-1	저장 데이터는 보호됩니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-1	저장 데이터는 보호됩니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-1	저장 데이터는 보호됩니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 대해 Key Management Service(AWS KMS)를 사용한 AWS 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-2	전송 중 데이터는 보호됩니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-2	전송 중 데이터는 보호됩니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-2	전송 중 데이터는 보호됩니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-2	전송 중 데이터는 보호됩니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-2	전송 중 데이터는 보호됩니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-2	전송 중 데이터는 보호됩니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-2	전송 중 데이터는 보호됩니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
PR.DS-2	전송 중 데이터는 보호됩니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-2	전송 중 데이터는 보호됩니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-3	자산의 제거, 이전 및 처분 과정이 공식적으로 관리됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-3	자산의 제거, 이전 및 처분 과정이 공식적으로 관리됩니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
PR.DS-3	자산의 제거, 이전 및 처분 과정이 공식적으로 관리됩니다.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
PR.DS-5	데이터 유출 방지 기능이 구현되었습니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 보안 인증 정보가 포함되지 않도록 합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능이 구현되었습니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-5	데이터 유출 방지 기능을 구현합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-6	무결성 검사 메커니즘은 소프트웨어, 펌웨어 및 정보 무결성을 확인하는 데 사용됩니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-6	무결성 검사 메커니즘은 소프트웨어, 펌웨어 및 정보 무결성을 확인하는 데 사용됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-7	개발 및 테스트 환경이 프로덕션 환경과 분리됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-7	개발 및 테스트 환경이 프로덕션 환경과 분리됩니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
PR.DS-7	개발 및 테스트 환경이 프로덕션 환경과 분리됩니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-7	개발 및 테스트 환경이 프로덕션 환경과 분리됩니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
PR.DS-7	개발 및 테스트 환경이 프로덕션 환경과 분리됩니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-7	개발 및 테스트 환경이 프로덕션 환경과 분리됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	account-part-of-organizations	Organizations AWS 계정 내 AWS 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-1	정보 기술 및 산업 제어 시스템의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 통합하여 생성 및 유지 관리됩니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-2	시스템 관리를 위한 시스템 개발 수명 주기를 구현합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.
PR.IP-2	시스템 관리를 위한 시스템 개발 수명 주기를 구현합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 보안 인증 정보가 포함되지 않도록 합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-2	시스템 관리를 위한 시스템 개발 수명 주기를 구현합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
PR.IP-3	구성 변경 제어 프로세스가 갖춰져 있습니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-3	구성 변경 제어 프로세스가 갖춰져 있습니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
PR.IP-4	정보 백업이 수행, 유지 및 테스트됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-7	보호 프로세스가 개선됩니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
PR.IP-8	보호 기술의 효과가 공유됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.IP-8	보호 기술의 효과가 공유됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-8	보호 기술의 효과가 공유됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.IP-8	보호 기술의 효과가 공유됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.IP-8	보호 기술의 효과가 공유됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-8	보호 기술의 효과가 공유됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.IP-8	보호 기술의 효과가 공유됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-8	보호 기술의 효과가 공유됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.IP-8	보호 기술의 효과가 공유됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.IP-8	보호 기술의 효과가 공유됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-8	보호 기술의 효과가 공유됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.IP-8	보호 기술의 효과가 공유됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-12	취약성 관리 계획이 개발되고 구현됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.IP-12	취약성 관리 계획이 개발되고 구현됩니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 확인할 수 있습니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하며 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 환경에 관한 기타 세부 정보의 기준선을 설정할 수 있도록 합니다.
PR.IP-12	취약성 관리 계획이 개발되고 구현됩니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.MA-2	조직 자산의 원격 유지 관리는 무단 액세스를 방지하는 방식으로 승인, 기록 및 수행됩니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.MA-2	조직 자산의 원격 유지 관리는 무단 액세스를 방지하는 방식으로 승인, 기록 및 수행됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	통신 및 제어 네트워크가 보호됩니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소, 이벤트 시간이 포함됩니다.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
PR.PT-1	감사 및 로그 기록은 정책에 따라 결정, 문서화, 구현 및 검토됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.PT-3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-4	통신 및 제어 네트워크가 보호됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-5	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RC.RP-1	사이버 보안 인시던트 발생 중 또는 이후에 복구 계획이 실행됩니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.AN-2	인시던트의 영향을 파악합니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.MI-3	새로 식별된 취약성은 완화되거나 허용되는 위험으로 문서화됩니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다 AWS . AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획의 AWS 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
RS.RP-1	사고 발생 중 또는 사고 발생 후에 대응 계획이 실행됩니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

템플릿

템플릿은 GitHub: NIST CSF 운영 모범 사례에서 확인할 수 있습니다.

NIST 개인정보보호 프레임워크 v1.0 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 NIST 개인정보보호 프레임워크와 AWS 관리형 Config 규칙 간의 샘플 매핑입니다. 각 AWS Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 NIST 프라이버시 프레임워크 제어와 관련이 있습니다. NIST 프라이버시 프레임워크 제어는 여러 AWS Config 규칙과 관련이 있을 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P7	데이터 요소와 관련된 처리 권한 및 관련 데이터 값을 전송하는 메커니즘이 확립되고 작동됩니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CT.DM-P7	데이터 요소와 관련된 처리 권한 및 관련 데이터 값을 전송하는 메커니즘이 확립되고 작동됩니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
CT.DM-P7	데이터 요소와 관련된 처리 권한 및 관련 데이터 값을 전송하는 메커니즘이 확립되고 작동됩니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사

제어 ID	제어 설명	AWS 구성 규칙	지침
			용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CT.DM-P7	데이터 요소와 관련된 처리 권한 및 관련 데이터 값을 전송하는 메커니즘이 확립되고 작동됩니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P7	데이터 요소와 관련된 처리 권한 및 관련 데이터 값을 전송하는 메커니즘이 확립되고 작동됩니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
CT.DM-P7	데이터 요소와 관련된 처리 권한 및 관련 데이터 값을 전송하는 메커니즘이 확립되고 작동됩니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P7	데이터 요소와 관련된 처리 권한 및 관련 데이터 값을 전송하는 메커니즘이 확립되고 작동됩니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CT.DM-P7	데이터 요소와 관련된 처리 권한 및 관련 데이터 값을 전송하는 메커니즘이 확립되고 작동됩니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
CT.DM-P7	데이터 요소와 관련된 처리 권한 및 관련 데이터 값을 전송하는 메커니즘이 확립되고 작동됩니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	audit-log-policy-exists(프로세스 확인)	조직의 로깅 요구 사항을 정의하는 감사 로그 관리 정책을 수립하고 유지 관리합니다. 여기에는 감사 로그의 검토 및 보존이 포함되며 이에 국한되지는 않습니다.
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail의 사용이 포함됩니다.
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
CT.DM-P8	감사 및 로그 기록은 정책에 따라 그리고 데이터 최소화 원칙을 적용하여 결정, 문서화, 구현 및 검토됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
ID.DE-P2	개인 정보 보호 위험 평가 프로세스를 사용하여 데이터 처리 생태계 당사자(예: 서비스 제공업체, 고객, 파트너, 제품 제조업체, 애플리케이션 개발자)를 식별하고 우선 순위를 지정하고 평가합니다.	annual-risk-assessment-performed(프로세스 확인)	조직에 대한 연간 위험 평가를 수행합니다. 위험 평가는 식별된 위험 및/또는 취약성이 조직에 영향을 미칠 가능성과 영향을 파악하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
PR.AC-P1	승인된 개인, 프로세스 및 장치에 대해 ID 및 보안 인증이 발급, 관리, 확인, 취소 및 감사를 거칩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-P3	원격 액세스가 관리됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-P3	원격 액세스가 관리됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
PR.AC-P3	원격 액세스가 관리됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
PR.AC-P3	원격 액세스가 관리됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-P3	원격 액세스가 관리됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.AC-P3	원격 액세스가 관리됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.AC-P3	원격 액세스가 관리됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
PR.AC-P3	원격 액세스가 관리됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P3	원격 액세스가 관리됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
PR.AC-P3	원격 액세스가 관리됩니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P4	액세스 권한 및 권한 부여는 최소 권한 및 업무 분리 원칙을 통합하여 관리됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
PR.AC-P5	네트워크 무결성이 보호됩니다(예: 네트워크 분리, 네트워크 분할).	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P6	개인과 디바이스는 인증을 받고 자격 증명에 구속되며, 거래 위험(예: 개인의 보안 및 개인 정보 보호 위험 및 기타 조직적 위험)에 상응하는 인증을 거칩니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
PR.AC-P6	개인과 디바이스는 인증을 받고 자격 증명에 구속되며, 거래 위험(예: 개인의 보안 및 개인 정보 보호 위험 및 기타 조직적 위험)에 상응하는 인증을 거칩니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P6	개인과 디바이스는 인증을 받고 자격 증명에 구속되며, 거래 위험(예: 개인의 보안 및 개인 정보 보호 위험 및 기타 조직적 위험)에 상응하는 인증을 거칩니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.AC-P6	개인과 디바이스는 인증을 받고 자격 증명에 구속되며, 거래 위험(예: 개인의 보안 및 개인 정보 보호 위험 및 기타 조직적 위험)에 상응하는 인증을 거칩니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
PR.AC-P6	개인과 디바이스는 인증을 받고 자격 증명에 구속되며, 거래 위험(예: 개인의 보안 및 개인 정보 보호 위험 및 기타 조직적 위험)에 상응하는 인증을 거칩니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P1	저장 데이터는 보호됩니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
PR.DS-P1	저장 데이터는 보호됩니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
PR.DS-P1	저장 데이터는 보호됩니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P1	저장 데이터는 보호됩니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-P1	저장 데이터는 보호됩니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
PR.DS-P1	저장 데이터는 보호됩니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P1	저장 데이터는 보호됩니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
PR.DS-P1	저장 데이터는 보호됩니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P1	저장 데이터는 보호됩니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-P1	저장 데이터는 보호됩니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-P1	저장 데이터는 보호됩니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P1	저장 데이터는 보호됩니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P1	저장 데이터는 보호됩니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-P1	저장 데이터는 보호됩니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P1	저장 데이터는 보호됩니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-P1	저장 데이터는 보호됩니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P1	저장 데이터는 보호됩니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-P1	저장 데이터는 보호됩니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P1	저장 데이터는 보호됩니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
PR.DS-P2	전송 중 데이터는 보호됩니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-P2	전송 중 데이터는 보호됩니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P2	전송 중 데이터는 보호됩니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
PR.DS-P2	전송 중 데이터는 보호됩니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P2	전송 중 데이터는 보호됩니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.DS-P4	가용성을 보장할 수 있는 충분한 용량이 유지됩니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
PR.DS-P5	데이터 유출 방지 기능을 구현합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.DS-P6	무결성 검사 메커니즘은 소프트웨어, 펌웨어 및 정보 무결성을 확인하는 데 사용됩니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.
PR.MA-P2	조직 자산의 원격 유지관리는 무단 액세스를 방지하는 방식으로 승인, 기록 및 수행됩니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.MA-P2	조직 자산의 원격 유지 관리는 무단 액세스를 방지하는 방식으로 승인, 기록 및 수행됩니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
PR.PO-P1	정보 기술의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 포함하여 생성되고 유지됩니다.	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하도록 하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P1	정보 기술의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 포함하여 생성되고 유지됩니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P1	정보 기술의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 포함하여 생성되고 유지됩니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
PR.PO-P1	정보 기술의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 포함하여 생성되고 유지됩니다.	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P1	정보 기술의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 포함하여 생성되고 유지됩니다.	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.
PR.PO-P1	정보 기술의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 포함하여 생성되고 유지됩니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P1	정보 기술의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 포함하여 생성되고 유지됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
PR.PO-P1	정보 기술의 기본 구성은 보안 원칙(예: 최소 기능 개념)을 포함하여 생성되고 유지됩니다.	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
AT-1: PR.PO-P10	취약성 관리 계획이 개발되고 구현됩니다.	vuln-management-plan-exists(프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 프로세스를 공식적으로 정의하려면 취약성 관리 계획을 개발하고 구현해야 합니다.
PR.PO-P2	구성 변경 제어 프로세스를 수립하고 실행합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
PR.PO-P2	구성 변경 제어 프로세스를 수립하고 실행합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이러한 최적화를 통해 인스턴스에서 Amazon EBS I/O 작업과 기타 트래픽 간의 경합이 최소화되어 EBS 볼륨의 성능이 극대화됩니다.
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.PO-P3	정보 백업이 수행, 유지 및 테스트됩니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.PO-P7	대응 계획(인시던트 대응 및 업무 연속성) 및 복구 계획(인시던트 복구 및 재해 복구)이 수립되고 시행되며 관리됩니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PO-P8	대응 및 복구 계획을 테스트합니다.	response-plan-tested(프로세스 확인)	사고 대응 및 복구 계획이 테스트되었는지 확인합니다. 이는 인시던트 발생 중에 해당 계획이 효과적인지 그리고 격차나 업데이트를 해결해야 하는지를 이해하는 데 도움이 될 수 있습니다.
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용되었습니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P2	필수 기능만 제공하도록 시스템을 구성함으로써 최소 기능의 원칙이 적용됩니다.	redshift-enhanced-vpc-routing-enabled	향상된 VPC 라우팅은 클러스터와 데이터 리포지토리 간의 모든 COPY 및 UNLOAD 트래픽이 Amazon VPC를 통과하도록 강제합니다. 그런 다음, 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수도 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift clusters can contain sensitive informati on and principles and access control is required for such accounts.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
PR.PT-P3	통신 및 제어 네트워크가 보호됩니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스에는 공개적으로 액세스할 수 없어야 합니다. 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새로운 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
PR.PT-P4	정상 및 부정적인 상황에서 복원력 요구 사항을 충족하기 위한 메커니즘(예: 페일세이프, 로드 밸런싱, 핫 스왑)이 구현됩니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

템플릿

템플릿은 GitHub: NIST 개인정보보호 프레임워크 v1.0 운영 모범 사례에서 확인할 수 있습니다.

NYDFS 23 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 금융 서비스 회사에 대한 뉴욕주 금융 서비스국(NYDFS) 사이버 보안 요구 사항(23 NYCRR 500)과 AWS 관리형 Config 규칙 간의 샘플 매핑입니다. 각 AWS Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 미국 NYDFS 제어와 관련이 있습니다. 미국 NYDFS 23 NYCRR 500 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요

제어 ID	제어 설명	AWS 구성 규칙	지침
	성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.		청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장되어 있을 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 강화된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.02(a)	(a) 사이버 보안 프로그램 각 적용 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 및 가용성을 보호하도록 설계된 사이버 보안 프로그램을 유지해야 합니다.	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(2)	(b) 사이버 보안 프로그램은 대상 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (2) 방어 인프라를 사용하고 정책 및 절차를 구현하여 해당 기관의 정보 시스템과 해당 정보 시스템에 저장된 비공개 정보를 무단 액세스, 사용 또는 기타 악의적 행위로부터 보호합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트 탐지.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(3)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (3) 사이버 보안 이벤트를 탐지합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.02(b)(5)	(b) 사이버 보안 프로그램은 해당 기관의 위험 평가를 기반으로 하며 다음과 같은 핵심 사이버 보안 기능을 수행하도록 설계되어야 합니다. (5) 사이버 보안 이벤트를 복구하고 정상 운영 및 서비스로 복원합니다.	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.05	각 대상 기관의 사이버 보안 프로그램에는 해당 기관의 위험 평가를 기반으로 개발된 모니터링 및 테스트가 포함되며, 이것들은 해당 기관의 사이버 보안 프로그램의 유효성을 평가하기 위해 고안되어야 합니다. 모니터링 및 테스트에는 지속적인 모니터링 또는 주기적인 침투 테스트 및 취약성 평가가 포함되어야 합니다. 취약성을 유발하거나 나타낼 수 있는 정보 시스템의 변화를 지속적으로 탐지하기 위한 효과적인 지속적 모니터링 또는 기타 시스템이 없는 경우, 해당 기관은 (a) 위험 평가에 따라 식별된 관련 위험을 기반으로 매년 결정되는 해당 주체의 정보 시스템에 대한 연간 침투 테스트 및 (b) 보안 취약성위험 평가에 기반한 해당 기관의 정보 시스템에 공개적으로 알려진 사이버 보안 취약성을 식별하도록 합리적으로 설계된 정보 시스템에	vuln-management-plan-exists(프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 공식적으로 정의된 프로세스를 보유할 수 있도록 취약성 관리 계획이 개발 및 구현되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
	대한 체계적인 스캔 또는 검토를 포함하여 연 2회 1회 취약성 평가를 실시해야 합니다.		
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(b)	(b) 각 대상 기관은 본 부의 섹션 500.06(a)(1)에서 요구하는 기록을 5년 이상 보관해야 하며, 본 부의 섹션 500.06(a)(2)에서 요구하는 기록을 3년 이상 보관해야 합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.06(a)	(a) 대상 기관은 해당하는 범위 내에서 위험 평가에 근거하여 다음과 같은 시스템을 안전하게 유지 관리해야 합니다. (1) 해당 기관의 정상적인 운영 및 의무를 지원하기에 충분한 중요 금융 거래를 재구성하도록 설계된 시스템 (2) 기관을 정상적으로 운영하는 데 중요한 부분을 실질적으로 해칠 가능성이 있는 사이버 보안 사건을 탐지하고 이에 대응하도록 설계된 감사 추적을 포함하는 시스템	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	ecs-task-definition-user-for-host-mode-check	작업 정의에 승격된 권한이 있는 경우는 고객이 해당 구성을 특별히 선택했기 때문입니다. 이 제어는 작업 정의에 호스트 네트워킹이 활성화되어 있지만 고객이 승격된 권한을 선택하지 않은 경우 예상치 못한 권한 에스컬레이션을 검사합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.07	사이버 보안 프로그램의 일환으로, 대상 기관의 위험 평가에 따라 각 대상 기관은 비공개 정보에 대한 액세스를 제공하는 정보 시스템에 대한 사용자 액세스 권한을 제한하고 이러한 액세스 권한을 정기적으로 검토해야 합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
500.8(a)	(a) 각 대상 기관의 사이버 보안 프로그램에는 해당 기관이 활용하는 자체 개발 애플리케이션에 대해 보안 개발 사례의 사용을 보장하기 위해 고안된 서면 절차, 지침 및 표준과 해당 기관의 기술 환경 내에서 활용하는 외부 개발 애플리케이션의 보안을 검토, 평가 또는 테스트하기 위한 절차가 포함되어야 합니다.	codebuild-project-envvar-awscred-check	인증 자격 증명 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 AWS Codebuild 프로젝트 환경 내에 존재하지 않는지 확인합니다. 이러한 변수를 일반 텍스트로 저장하지 마세요. 이러한 변수를 일반 텍스트로 저장하면 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.8(a)	(a) 각 대상 기관의 사이버 보안 프로그램에는 해당 기관이 활용하는 자체 개발 애플리케이션에 대해 보안 개발 사례의 사용을 보장하기 위해 고안된 서면 절차, 지침 및 표준과 해당 기관의 기술 환경 내에서 활용하는 외부 개발 애플리케이션의 보안을 검토, 평가 또는 테스트하기 위한 절차가 포함되어야 합니다.	codebuild-project-source-repo-url-check	GitHub 또는 Bitbucket 소스 리포지토리 URL에 AWS Codebuild 프로젝트 환경 내의 개인 액세스 토큰, 로그인 자격 증명이 포함되어 있지 않은지 확인합니다. 개인 액세스 토큰이나 로그인 보안 인증 정보 대신 OAuth를 사용하여 GitHub 또는 Bitbucket 리포지토리에 액세스할 수 있는 권한을 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.09	(a) 각 대상 기관은 본부에서 요구하는 대로 사이버 보안 프로그램이 설계되었음을 알리기에 충분하도록 해당 기관의 정보 시스템에 대한 정기적인 위험 평가를 실시해야 합니다. 이러한 위험 평가는 해당 기관의 정보 시스템, 미공개정보 또는 비즈니스 운영의 변경 사항을 다루기 위해 합리적으로 필요한 경우 업데이트되어야 합니다. 대상 기관의 위험 평가는 기술 발전 및 진화하는 위협에 대응하기 위한 제어 수정이 가능해야 합니다. 또한 사이버 보안, 비공개 정보 수집 또는 저장, 정보 시스템 활용과 같은 대상 기관의 사업 운영과 관련된 특정 위험 그리고 비공개 정보 및 정보 시스템을 보호하기 위한 제어 수단의 가용성 및 유효성를 고려해야 합니다.	annual-risk-assessment-performed(프로세스 확인)	조직에 대한 연간 위험 평가를 수행합니다. 위험 평가는 식별된 위험 및/또는 취약성이 조직에 영향을 미칠 가능성과 영향을 파악하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.12	(a) 다중 인증 위험 평가에 따라 각 대상 기관은 비공개 정보 또는 정보 시스템에 대한 무단 접근을 방지하기 위해 다중 인증 또는 위험 기반 인증을 포함한 효과적인 제어 수단을 사용해야 합니다. (b) 외부 네트워크를 통해 대상 기관의 내부 네트워크에 접속하는 개인에 대해서는 다단계 인증을 사용해야 합니다. 단, 해당 기관의 CISO(Chief Information Security Officer)가 합리적으로 동등하거나 더 안전한 액세스 제어의 사용을 서면으로 승인한 경우는 예외입니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.12	(a) 다중 인증 위험 평가에 따라 각 대상 기관은 비공개 정보 또는 정보 시스템에 대한 무단 접근을 방지하기 위해 다중 인증 또는 위험 기반 인증을 포함한 효과적인 제어 수단을 사용해야 합니다. (b) 외부 네트워크를 통해 대상 기관의 내부 네트워크에 접속하는 개인에 대해서는 다단계 인증을 사용해야 합니다. 단, 해당 기관의 CISO(Chief Information Security Officer)가 합리적으로 동등하거나 더 안전한 액세스 제어의 사용을 서면으로 승인한 경우는 예외입니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.12	(a) 다중 인증 위험 평가에 따라 각 대상 기관은 비공개 정보 또는 정보 시스템에 대한 무단 접근을 방지하기 위해 다중 인증 또는 위험 기반 인증을 포함한 효과적인 제어 수단을 사용해야 합니다. (b) 외부 네트워크를 통해 대상 기관의 내부 네트워크에 접속하는 개인에 대해서는 다단계 인증을 사용해야 합니다. 단, 해당 기관의 CISO(Chief Information Security Officer)가 합리적으로 동등하거나 더 안전한 액세스 제어의 사용을 서면으로 승인한 경우는 예외입니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.12	(a) 다중 인증 위험 평가에 따라 각 대상 기관은 비공개 정보 또는 정보 시스템에 대한 무단 접근을 방지하기 위해 다중 인증 또는 위험 기반 인증을 포함한 효과적인 제어 수단을 사용해야 합니다. (b) 외부 네트워크를 통해 대상 기관의 내부 네트워크에 접속하는 개인에 대해서는 다단계 인증을 사용해야 합니다. 단, 해당 기관의 CISO(Chief Information Security Officer)가 합리적으로 동등하거나 더 안전한 액세스 제어의 사용을 서면으로 승인한 경우는 예외입니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.12	(a) 다중 인증 위험 평가에 따라 각 대상 기관은 비공개 정보 또는 정보 시스템에 대한 무단 접근을 방지하기 위해 다중 인증 또는 위험 기반 인증을 포함한 효과적인 제어 수단을 사용해야 합니다. (b) 외부 네트워크를 통해 대상 기관의 내부 네트워크에 접속하는 개인에 대해서는 다단계 인증을 사용해야 합니다. 단, 해당 기관의 CISO(Chief Information Security Officer)가 합리적으로 동등하거나 더 안전한 액세스 제어의 사용을 서면으로 승인한 경우는 예외입니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	cloudwatch-alarm-action-check	지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 Amazon CloudWatch 경보를 통해 경고합니다. 이러한 경보는 여러 기간에 대해 지정된 임계값과 지표 또는 표현식의 값을 비교하여 하나 이상의 작업을 수행합니다. 이 규칙에는 alarmActionRequired(Config 기본값: True), insufficientDataActionRequired(Config 기본값: True), okActionRequired(Config 기본값: False)에 대한 값이 필요합니다. 실제 값은 사용자 환경의 경보 동작을 반영해야 합니다.
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.
500.14(a)	(a) 승인된 사용자의 활동을 모니터링하고 승인되지 않은 사용자가 비공개 정보를 무단 액세스, 사용 또는 변조하는 것을 탐지하도록 설계된 위험 기반 정책, 절차 및 제어를 구현합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
500.14(b)	사이버 보안 프로그램의 일환으로 각 대상 기관은 (b) 모든 직원에게 정기적인 사이버 보안 인식 교육을 제공해야 하며, 이러한 교육은 해당 주체가 위험 평가에서 식별한 위험을 반영하도록 업데이트해야 합니다.	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 민감한 데이터가 저장되어 있을 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.
500.15(a)	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 위험 평가에 따라 외부 네트워크를 통해 전송 중인 정보와 저장 중인 정보 모두에 대해 해당 기관이 보유하거나 전송하는 비공개 정보를 보호하기 위해 암호화를 포함한 제어 수단을 구현해야 합니다.	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
500.16	(a) 사이버 보안 프로그램의 일환으로, 각 대상 기관은 해당 기관의 정보 시스템의 기밀성, 무결성 혹은 가용성 또는 비즈니스 혹은 운영의 모든 측면에 있어서 지속적인 기능에 중대한 영향을 미치는 사이버 보안 사건에 신속하게 대응하고 복구할 수 있도록 설계된 서면 사고 대응 계획을 수립해야 합니다.	response-plan-exists-maintained(프로세스 확인)	인시던트 대응 계획이 수립, 유지 관리되고 담당 직원에게 배포되는지 확인합니다.

템플릿

템플릿은 GitHub: NYDFS 23 운영 모범 사례에서 확인할 수 있습니다.

NZISM 3.8 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙과 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 뉴질랜드 정부 통신 보안국(GCSB) 정보 보안 매뉴얼(NZISM) 2022-09 버전 3.8과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스 유형에 적용되며 하나 이상의 NZISM 제어와 관련이 있습니다. NZISM 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요. 제한됨 이하로 분류된 정보에 대한 권장 또는 기준 관행을 나타내는 제어만 매핑에 포함됩니다.

이 샘플 적합성 팩 템플릿에는 인력, 정보 및 물리적 보안 관리에 대한 뉴질랜드 정부의 기대치를 규정하는 보호 보안 요구 사항(PSR) 프레임워크의 필수 부분인 NZISM 프레임워크 내 제어에 대한 매핑이 포함되어 있습니다.

NZISM은 크리에이티브 커먼즈 저작자표시 4.0 뉴질랜드 라이선스에 따라 이용할 수 있으며, https://creativecommons.org/licenses/by/4.0/에서 확인할 수 있습니다. 저작권 정보는 NZISM New Zealand Information Security Manual | Legal, Privacy, and Copyright에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1149	소프트웨어 보안, 표준 운영 환경, 강화된 SOEs 개발(14.1.8.C.01.)	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 자세한 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
1149	소프트웨어 보안, 표준 운영 환경, 강화된 SOEs 개발(14.1.8.C.01.)	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어

제어 ID	제어 설명	AWS 구성 규칙	지침
			설치, 애플리케이션 구성 및 환경에 대한 기타 세부 정보의 기준을 설정할 수 있습니다.
1149	소프트웨어 보안, 표준 운영 환경, 강화된 SOEs 개발(14.1.8.C.01.)	ecs-containers-nonprivileged	이 제어는 Amazon ECS 작업 정의의 컨테이너 정의에 있는 권한 있는 파라미터가 true로 설정되어 있는지 확인합니다. 이 파라미터가 true와 같으면 제어가 실패합니다. 이 제어는 Amazon ECS 작업 정의의 최신 활성 개정만 평가합니다. ECS 태스크 정의에서 상승된 권한을 제거하는 것이 좋습니다. 권한 파라미터가 true이면 컨테이너에 호스트 컨테이너 인스턴스에 대한 승격된 권한이 부여됩니다(루트 사용자와 유사).

제어 ID	제어 설명	AWS 구성 규칙	지침
1149	소프트웨어 보안, 표준 운영 환경, 강화된 SOEs 개발(14.1.8.C.01.)	ecs-containers-readonly-access	이 제어는 Amazon ECS 컨테이너가 마운트된 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되는지 확인합니다. Amazon ECS 태스크 정의의 컨테이너 정의에 있는 ReadonlyRootFilesystem 파라미터가 false로 설정된 경우이 제어가 실패합니다. 이 제어는 Amazon ECS 작업 정의의 최신 활성 개정만 평가합니다. 이 옵션을 활성화하면 파일 시스템 폴더 및 디렉터리에 대한 명시적인 읽기-쓰기 권한이 없는 한 컨테이너 인스턴스의 파일 시스템을 조작하거나 쓸 수 없으므로 보안 공격 벡터가 줄어듭니다. 이 제어는 또한 최소 권한 원칙을 준수합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1661	소프트웨어 보안, 웹 애플리케이션 개발, 에이전트 웹 사이트 콘텐츠(14.5.6.C.01.)	cloudfront-default-root-object-configured	이 제어는 Amazon CloudFront 배포가 기본 루트 객체인 특정 객체를 반환하도록 구성되어 있는지 여부를 확인합니다. CloudFront 배포에 기본 루트 객체가 구성되어 있지 않으면 제어가 실패합니다. 사용자가 배포의 객체 대신 배포의 루트 URL을 요청하는 경우가 있습니다. 이 경우, 기본 루트 객체를 지정하면 웹 배포 내용이 노출되는 것을 방지하는 데 도움이 될 수 있습니다. us-east-1 리전에서는 이 규칙을 반드시 적용해야 합니다. 템플릿 파라미터 DeployEdgeRules = true를 사용하여 배포

제어 ID	제어 설명	AWS 구성 규칙	지침
1667	소프트웨어 보안, 웹 애플리케이션 개발, 웹 애플리케이션(14.5.8.C.01.)	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration에 대한 값이 필요합니다. 값은 90일입니다.
1667	소프트웨어 보안, 웹 애플리케이션 개발, 웹 애플리케이션(14.5.8.C.01.)	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1841	액세스 제어 및 암호, 식별, 인증 및 암호, 시스템 사용자 식별 및 인증 방법(16.1.35.C.02.)	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1841	액세스 제어 및 암호, 식별, 인증 및 암호, 시스템 사용자 식별 및 인증 방법(16.1.35.C.02.)	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1841	액세스 제어 및 암호, 식별, 인증 및 암호, 시스템 사용자 식별 및 인증 방법(16.1.35.C.02.)	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 AWS 계정에서 가장 권한이 있는 사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 AWS 계정의 인시던트를 줄일 수 있습니다.
1841	액세스 제어 및 암호, 식별, 인증 및 암호, 시스템 사용자 식별 및 인증 방법(16.1.35.C.02.)	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 AWS 계정에서 가장 권한이 있는 사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 AWS 계정의 인시던트를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1847	액세스 제어 및 암호, 식별, 인증 및 암호, 전송 중 인증 데이터 보호(16.1.37.C.01.)	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1847	액세스 제어 및 암호, 식별, 인증 및 암호, 전송 중 인증 데이터 보호(16.1.37.C.01.)	cloudfront-viewer-policy-https	이 제어는 Amazon CloudFront 배포에서 뷰어가 HTTPS를 직접 사용하도록 요구하는지 또는 리디렉션을 사용하는지 여부를 확인합니다. ViewerProtocolPolicy가 defaultCacheBehavior 또는 cacheBehaviors에 대해 allow-all로 설정된 경우 제어가 실패합니다. HTTPS(TLS)를 사용하여 잠재적 공격자가 중간자 또는 그와 유사한 공격을 사용하여 네트워크 트래픽을 염탐하거나 조작하지 못하게 할 수 있습니다. 암호화된 HTTPS(TLS) 연결만 허용되어야 합니다. us-east-1 리전에서는 이 규칙을 반드시 적용해야 합니다. 템플릿 파라미터 DeployEdgeRules = true를 사용하여 배포

제어 ID	제어 설명	AWS 구성 규칙	지침
1847	액세스 제어 및 암호, 식별, 인증 및 암호, 전송 중 인증 데이터 보호(16.1.37.C.01.)	elasticsearch-node-to-node-encryption-check	이 제어는 Elasticsearch 도메인에 노드 간 암호화를 활성화하고 있는지 확인합니다. 도메인에서 노드 간 암호화를 비활성화하면 이 제어가 실패합니다. HTTPS(TLS)를 사용하면 잠재적인 공격자가 중간자 또는 유사한 공격을 통해 네트워크 트래픽을 도청하거나 조작하는 것을 방지할 수 있습니다. HTTPS(TLS)를 통한 암호화된 연결만 허용되어야 합니다. Elasticsearch 도메인의 노드 간 암호화를 활성화하면 클러스터 내 통신이 전송 중 암호화됩니다.
1847	액세스 제어 및 암호, 식별, 인증 및 암호, 전송 중 인증 데이터 보호(16.1.37.C.01.)	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1847	액세스 제어 및 암호, 식별, 인증 및 암호, 전송 중 인증 데이터 보호(16.1.37.C.01.)	opensearch-node-to-node-encryption-check	이 제어는 OpenSearch 도메인에 노드 간 암호화가 활성화되어 있는지 확인합니다. 도메인에서 노드 간 암호화를 비활성화하면 이 제어가 실패합니다. HTTPS(TLS)를 사용하면 잠재적인 공격자가 중간자 또는 유사한 공격을 통해 네트워크 트래픽을 도청하거나 조작하는 것을 방지할 수 있습니다. HTTPS(TLS)를 통한 암호화된 연결만 허용되어야 합니다. OpenSearch 도메인에 대해 노드 간 암호화를 활성화하면 클러스터 내 통신이 전송 중 암호화됩니다.
1858	액세스 제어 및 암호, 식별, 인증 및 암호, 암호 선택 정책(16.1.40.C.02.)	iam-password-policy	HTTPS(TLS)를 사용하여 잠재적 공격자가 중간자 또는 그와 유사한 공격을 사용하여 네트워크 트래픽을 염탐하거나 조작하지 못하게 할 수 있습니다. 암호화된 HTTPS(TLS) 연결만 허용되어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1893	액세스 제어 및 암호, 식별, 인증 및 암호, 액세스 일시 중지(16.1.46.C.02.)	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙은 maxCredentialUsageAge를 30일로 설정합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1946	액세스 제어 및 암호, 권한 있는 사용자 액세스, 권한 있는 계정 사용(16.3.5.C.02.)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
1946	액세스 제어 및 암호, 권한 있는 사용자 액세스, 권한 있는 계정 사용(16.3.5.C.02.)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정을 생성하고 사용하여 최소 기능 원칙을 통합할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1998	액세스 제어 및 암호, 이벤트 로깅 및 감사, 시스템 관리 로그 유지 관리(16.6.6.C.02.)	cloud-trail-cloud-watch-logs-enabled	추적 로그를 모니터링하고 특정 활동이 발생할 때 알림을 받도록 CloudWatch Logs로 CloudTrailCloudTrail을 구성해야 합니다. 이 규칙은 AWS CloudTrail 추적이 Amazon CloudWatch logs 로그로 로그를 전송하도록 구성되어 있는지 확인합니다.
1998	액세스 제어 및 암호, 이벤트 로깅 및 감사, 시스템 관리 로그 유지 관리(16.6.6.C.02.)	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1998	액세스 제어 및 암호, 이벤트 로깅 및 감사, 시스템 관리 로그 유지 관리(16.6.6.C.02.)	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다. 최소 보존 기간은 18개월입니다.
2013	액세스 제어 및 암호, 이벤트 로깅 및 감사, 로깅할 추가 이벤트 (16.6.10.C.02)	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2013	액세스 제어 및 암호, 이벤트 로깅 및 감사, 로깅할 추가 이벤트 (16.6.10.C.02)	cloudfront-accesslogs-enabled	이 제어는 CloudFront 배포에서 서버 액세스 로깅이 활성화되었는지 여부를 확인합니다. 배포에 대한 액세스 로깅이 활성화되지 않은 경우, 제어가 실패합니다. CloudFront 액세스 로그는 CloudFront가 수신하는 모든 사용자 요청에 대한 세부 정보를 제공합니다. 각 로그에는 요청이 수신된 날짜 및 시간, 요청한 뷰어의 IP 주소, 요청 소스, 뷰어의 요청 포트 번호 등의 정보가 포함됩니다. 이러한 로그는 보안 및 액세스 감사, 포렌식 조사와 같은 목적에 유용합니다. us-east-1 리전에서는 이 규칙을 반드시 적용해야 합니다. 템플릿 파라미터 DeployEdgeRules = true를 사용하여 배포

제어 ID	제어 설명	AWS 구성 규칙	지침
2013	액세스 제어 및 암호, 이벤트 로깅 및 감사, 로깅할 추가 이벤트 (16.6.10.C.02)	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
2013	액세스 제어 및 암호, 이벤트 로깅 및 감사, 로깅할 추가 이벤트 (16.6.10.C.02)	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2013	액세스 제어 및 암호, 이벤트 로깅 및 감사, 로깅할 추가 이벤트 (16.6.10.C.02)	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
2013	액세스 제어 및 암호, 이벤트 로깅 및 감사, 로깅할 추가 이벤트 (16.6.10.C.02)	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2022	액세스 제어 및 암호, 이벤트 로깅 및 감사, 이벤트 로그 보호 (16.6.12.C.01.)	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
2022	액세스 제어 및 암호, 이벤트 로깅 및 감사, 이벤트 로그 보호 (16.6.12.C.01.)	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
2028	액세스 제어 및 암호, 이벤트 로깅 및 감사, 이벤트 로그 아카이브 (16.6.13.C.01.)	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다. 최소 보존 기간은 18개월입니다.
2082	암호화, 암호화 기본 사항, 스토리지 및 물리적 전송 요구 사항 감소(17.1.53.C.04.)	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다. 사전 프로덕션 환경에는 예외가 적용됩니다.
2082	암호화, 암호화 기본 사항, 스토리지 및 물리적 전송 요구 사항 감소(17.1.53.C.04.)	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2082	암호화, 암호화 기본 사항, 스토리지 및 물리적 전송 요구 사항 감소(17.1.53.C.04.)	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2082	암호화, 암호화 기본 사항, 스토리지 및 물리적 전송 요구 사항 감소(17.1.53.C.04.)	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2082	암호화, 암호화 기본 사항, 스토리지 및 물리적 전송 요구 사항 감소(17.1.53.C.04.)	elasticsearch-encrypted-at-rest	이 제어는 Elasticsearch 도메인encryption-at-rest 구성이 활성화되어 있는지 확인합니다. 유휴 시 암호화가 활성화되지 않은 경우, 이 확인이 실패합니다. 민감한 데이터에 대한 보안 계층을 추가하려면 저장 시 암호화되도록 Elasticsearch Service 도메인을 구성해야 합니다. 저장 데이터의 암호화를 구성하면 AWS KMS는 암호화 키를 저장하고 관리합니다. 암호화를 수행하기 위해 AWS KMS는 256비트 키(AES-256)와 함께 고급 암호화 표준 알고리즘을 사용합니다.
2082	암호화, 암호화 기본 사항, 스토리지 및 물리적 전송 요구 사항 감소(17.1.53.C.04.)	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2082	암호화, 암호화 기본 사항, 스토리지 및 물리적 전송 요구 사항 감소(17.1.53.C.04.)	opensearch-encrypted-at-rest	이 제어는 OpenSearch 도메인에 저장 시 암호화 구성이 활성화되어 있는지 확인합니다. 유휴 시 암호화가 활성화되지 않은 경우, 이 확인이 실패합니다. 중요한 데이터에 대한 보안 계층을 추가하려면 OpenSearch Service 도메인이 저장 시 암호화되도록 구성해야 합니다. 저장 데이터의 암호화를 구성하면 AWS KMS는 암호화 키를 저장하고 관리합니다. 암호화를 수행하기 위해 AWS KMS는 256비트 키(AES-256)와 함께 고급 암호화 표준 알고리즘을 사용합니다.
2082	암호화, 암호화 기본 사항, 스토리지 및 물리적 전송 요구 사항 감소(17.1.53.C.04.)	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2082	암호화, 암호화 기본 사항, 스토리지 및 물리적 전송 요구 사항 감소(17.1.53.C.04.)	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2082	암호화, 암호화 기본 사항, 스토리지 및 물리적 전송 요구 사항 감소(17.1.53.C.04.)	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2082	암호화, 암호화 기본 사항, 스토리지 및 물리적 전송 요구 사항 감소(17.1.53.C.04.)	s3-default-encryption-kms	저장 데이터를 보호하려면 S3 버킷에 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다. 암호화 프로세스 및 관리에 대한 자세한 내용은 AWS Key Management Service(AWS KMS) 고객 관리형 CMKs 사용합니다. SSE가 활성화된 경우 민감하지 않은 데이터가 포함된 버킷에 대해 공제를 사용할 수 있습니다.
2090	암호화, 암호화 기본 사항, 정보 및 시스템 보호(17.1.55.C.02.)	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2090	암호화, 암호화 기본 사항, 정보 및 시스템 보호(17.1.55.C.02.)	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2090	암호화, 암호화 기본 사항, 정보 및 시스템 보호(17.1.55.C.02.)	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2598	암호화, 전송 계층 보안, TLS 사용(17.4.16.C.01.)	elb-custom-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic ElasticLoadBalancer SSL 리스너가 사용자 지정 보안 정책을 사용하고 있는지 확인합니다. 이러한 정책은 시스템 간 암호화된 네트워크 통신을 보장하는 데 도움이 되는 다양한 고강도 암호화 알고리즘을 제공할 수 있습니다. 이 규칙을 사용하려면 SSL 리스너에 대한 사용자 지정 보안 정책을 설정해야 합니다. 보안 정책은 Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256.

제어 ID	제어 설명	AWS 구성 규칙	지침
2600	암호화, 전송 계층 보안, TLS 사용(17.4.16.C.02.)	elb-custom-security-policy-ssl-check	전송 중 데이터를 보호하려면 Classic ElasticLoadBalancer SSL 리스너가 사용자 지정 보안 정책을 사용하고 있는지 확인합니다. 이러한 정책은 시스템 간 암호화된 네트워크 통신을 보장하는 데 도움이 되는 다양한 고강도 암호화 알고리즘을 제공할 수 있습니다. 이 규칙을 사용하려면 SSL 리스너에 대한 사용자 지정 보안 정책을 설정해야 합니다. 기본 보안 정책은 Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2726	암호화, 보안 쉘, 자동 원격 액세스(17.5.8.C.02.)	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 수신 및 송신 네트워크 트래픽의 상태 저장 필터링을 제공하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3021	암호화, 키 관리, KMPs 콘텐츠(17.9.25.C.01.)	cmk-backing-key-rotation-enabled	AWS KMS를 사용하면 고객이 KMS에 저장된 키 구성 요소이며 CMK의 키 ID에 AWS 연결된 지원 키를 교체할 수 있습니다. 이 백업 키는 암호화, 해독 등 암호화 작업을 수행하는 데 사용됩니다. 자동화된 키 교체는 암호화된 데이터의 해독이 투명하게 이루어질 수 있도록 하기 위해 현재 모든 이전 버전의 백업 키를 유지합니다. 암호화 키를 교체하면 노출되었을 수 있는 이전 키로 새로운 키로는 암호화된 데이터에 액세스할 수 없으므로 침해된 키가 영향을 미칠 가능성을 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3205	네트워크 보안, 네트워크 관리, 네트워크 액세스 제한(18.1.13.C.02.)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다. 승인된 인터넷 포트 목록은 443 전용입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3449	제품 보안, 제품 패치 적용 및 업데이트, 제품의 취약성 패치 적용 (12.4.4.C.02.)	ec2-managedinstance-patch-compliance-status-check	Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 되는 규칙을 활성화합니다. 이 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3449	제품 보안, 제품 패치 적용 및 업데이트, 제품의 취약성 패치 적용 (12.4.4.C.02.)	ecr-private-image-scanning-enabled	이 제어는 프라이빗 ECR 리포지토리에 이미지 스캔이 구성되어 있는지 확인합니다. 프라이빗 ECR 리포지토리에 이미지 스캔이 구성되어 있지 않으면이 제어가 실패합니다. 또한이 제어를 전달하려면 각 리포지토리에 대해 푸시 시 스캔을 구성해야 합니다. ECR 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR은 오픈 소스 Clair 프로젝트의 CVE(일반적인 취약성 및 노출) 데이터베이스를 사용하고 스캔 조사 결과 목록을 제공합니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3449	제품 보안, 제품 패치 적용 및 업데이트, 제품의 취약성 패치 적용 (12.4.4.C.02.)	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙은 allowVersionUpgrade를 TRUE로 설정합니다.
3451	제품 보안, 제품 패치 적용 및 업데이트, 제품의 취약성 패치 적용 (12.4.4.C.04.)	ec2-managedinstance-patch-compliance-status-check	Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 되는 규칙을 활성화합니다. 이 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3452	제품 보안, 제품 패치 적용 및 업데이트, 제품의 취약성 패치 적용 (12.4.4.C.05.)	ec2-managedinstance-patch-compliance-status-check	Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 되는 규칙을 활성화합니다. 이 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
3452	제품 보안, 제품 패치 적용 및 업데이트, 제품의 취약성 패치 적용 (12.4.4.C.05.)	elastic-beanstalk-managed-updates-enabled	이 제어는 Elastic Beanstalk 환경에 대해 관리형 플랫폼 업데이트가 활성화되었는지 여부를 확인합니다. 관리형 플랫폼 업데이트를 활성화하면 해당 환경에 사용 가능한 최신 플랫폼 수정 사항, 업데이트 및 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것은 시스템 보안의 중요한 단계입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3452	제품 보안, 제품 패치 적용 및 업데이트, 제품의 취약성 패치 적용 (12.4.4.C.05.)	rds-automatic-minor-version-upgrade-enabled	이 제어는 RDS 데이터베이스 인스턴스에 대해 자동 마이너 버전 업그레이드가 활성화되어 있는지 확인합니다. 자동 마이너 버전 업그레이드를 활성화하면 관계형 데이터베이스 관리 시스템(RDBMS)에 대한 최신 마이너 버전 업데이트가 설치됩니다. 이러한 업그레이드에는 보안 패치 및 버그 수정이 포함될 수 있습니다. 패치 설치를 최신 상태로 유지하는 것은 시스템 보안의 중요한 단계입니다.
3453	제품 보안, 제품 패치 적용 및 업데이트, 제품의 취약성 패치 적용 (12.4.4.C.06.)	ec2-managedinstance-patch-compliance-status-check	Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 되는 규칙을 활성화합니다. 이 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3453	제품 보안, 제품 패치 적용 및 업데이트, 제품의 취약성 패치 적용 (12.4.4.C.06.)	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙은 allowVersionUpgrade를 TRUE로 설정합니다.
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다. 로드 밸런서가 WAF가 활성화된 CloudFront 배포의 오리진인 경우 예외를 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	api-gw-associated-with-waf	이 제어는 API Gateway 단계에서 AWS WAF 웹 액세스 제어 목록(ACL)을 사용하는지 확인합니다. AWS WAF 리전 웹 ACL이 REST API Gateway 단계에 연결되지 않은 경우이 제어가 실패합니다. AWS WAF는 웹 애플리케이션과 APIs를 공격으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 이를 통해 사용자 정의 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 집합인 ACL을 구성할 수 있습니다. API Gateway 단계가 AWS WAF 웹 ACL과 연결되어 있는지 확인하여 악의적인 공격으로부터 보호합니다. API Gateway가 WAF가 활성화된 CloudFront 배포의 오리진인 경우 예외를 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	cloudfront-associated-with-waf	이 제어는 CloudFront 배포가 AWS WAF 또는 AWS WAFv2 웹 ACLs과 연결되어 있는지 확인합니다. 배포가 웹 ACL과 연결되지 않은 경우 제어가 실패합니다. AWS WAF는 웹 애플리케이션 및 APIs으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 사용자가 정의한 맞춤형 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 집합(웹 액세스 제어 목록 또는 웹 ACL)을 구성할 수 있습니다. CloudFront 배포가 AWS WAF 웹 ACL과 연결되어 있는지 확인하여 악의적인 공격으로부터 보호합니다. us-east-1 리전에서는 이 규칙을 반드시 적용해야 합니다. 템플릿 파라미터 DeployEdgeRules = true를 사용하여 배포

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	elasticsearch-in-vpc-only	이 제어는 Elasticsearch 도메인이 VPC에 있는지 확인합니다. 퍼블릭 액세스를 확인하기 위해 VPC 서브넷 라우팅 구성을 평가하지 않습니다. Elasticsearch 도메인이 퍼블릭 서브넷에 연결되어 있지 않은지 확인해야 합니다. VPC 내에 배포된 Elasticsearch 도메인은 퍼블릭 인터넷을 통과할 필요 없이 프라이빗 AWS 네트워크를 통해 VPC 리소스와 통신할 수 있습니다. 이 구성은 전송 중 데이터에 대한 액세스를 제한하여 보안 상태를 강화합니다. VPCs 네트워크 ACL 및 보안 그룹을 포함하여 Elasticsearch 도메인에 대한 액세스를 보호하기 위한 여러 네트워크 제어를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty 는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	opensearch-in-vpc-only	이 제어는 OpenSearch 도메인이 VPC에 있는지 확인합니다. 퍼블릭 액세스를 확인하기 위해 VPC 서브넷 라우팅 구성을 평가하지 않습니다. OpenSearch 도메인이 퍼블릭 서브넷에 연결되어 있지 않은지 확인해야 합니다. VPC 내에 배포된 OpenSearch 도메인은 퍼블릭 인터넷을 통과할 필요 없이 프라이빗 AWS 네트워크를 통해 VPC 리소스와 통신할 수 있습니다. 이 구성은 전송 중 데이터에 대한 액세스를 제한하여 보안 상태를 강화합니다. VPC는 네트워크 ACL 및 보안 그룹을 포함하여 OpenSearch 도메인에 대한 액세스를 보호하기 위한 다양한 네트워크 제어를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	rds-instance-public-access-check	Amazon Relational Database Service(RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙은 ignorePublicAcls를 TRUE로, blockPublicPolicy를 TRUE로, blockPublicAcls를 TRUE로, restrictPublicBuckets를 TRUE로 설정합니다.
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북이 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 수신 및 송신 네트워크 트래픽의 상태 저장 필터링을 제공하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
3562	게이트웨이 보안, 게이트웨이, 게이트웨이 구성(19.1.12.C.01.)	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3623	게이트웨이 보안, 게이트웨이, 비무장 영역 (19.1.14.C.02.)	elasticsearch-in-vpc-only	이 제어는 Elasticsearch 도메인이 VPC에 있는지 확인합니다. 퍼블릭 액세스를 확인하기 위해 VPC 서브넷 라우팅 구성을 평가하지 않습니다. Elasticsearch 도메인이 퍼블릭 서브넷에 연결되어 있지 않은지 확인해야 합니다. VPC 내에 배포된 Elasticsearch 도메인은 퍼블릭 인터넷을 통과할 필요 없이 프라이빗 AWS 네트워크를 통해 VPC 리소스와 통신할 수 있습니다. 이 구성은 전송 중 데이터에 대한 액세스를 제한하여 보안 상태를 강화합니다. VPCs 네트워크 ACL 및 보안 그룹을 포함하여 Elasticsearch 도메인에 대한 액세스를 보호하기 위한 여러 네트워크 제어를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3623	게이트웨이 보안, 게이트웨이, 비무장 영역 (19.1.14.C.02.)	opensearch-in-vpc-only	이 제어는 OpenSearch 도메인이 VPC에 있는지 확인합니다. 퍼블릭 액세스를 확인하기 위해 VPC 서브넷 라우팅 구성을 평가하지 않습니다. OpenSearch 도메인이 퍼블릭 서브넷에 연결되어 있지 않은지 확인해야 합니다. VPC 내에 배포된 OpenSearch 도메인은 퍼블릭 인터넷을 통과할 필요 없이 프라이빗 AWS 네트워크를 통해 VPC 리소스와 통신할 수 있습니다. 이 구성은 전송 중 데이터에 대한 액세스를 제한하여 보안 상태를 강화합니다. VPC는 네트워크 ACL 및 보안 그룹을 포함하여 OpenSearch 도메인에 대한 액세스를 보호하기 위한 다양한 네트워크 제어를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3623	게이트웨이 보안, 게이트웨이, 비무장 영역 (19.1.14.C.02.)	rds-instance-public-access-check	Amazon Relational Database Service(RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
3623	게이트웨이 보안, 게이트웨이, 비무장 영역 (19.1.14.C.02.)	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3815	네트워크 보안, 침입 탐지 및 방지, IDS/IPS 유지 관리(18.4.9.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
3857	네트워크 보안, 침입 탐지 및 방지, IDS/IPS 구성(18.4.11.C.01.)	guardduty-eks-protection-audit-enabled	이 제어는 GuardDuty EKS 감사 로그 모니터링이 활성화되어 있는지 확인합니다. EKS 감사 로그 모니터링을 사용하면 Amazon Elastic Kubernetes Service(Amazon EKS)의 EKS 클러스터에서 잠재적으로 의심스러운 활동을 탐지할 수 있습니다. EKS 감사 로그 모니터링은 Kubernetes 감사 로그를 사용하여 사용자, Kubernetes API를 사용하는 애플리케이션, 컨트롤 플레인의 시간순 활동을 캡처합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3857	네트워크 보안, 침입 탐지 및 방지, IDS/IPS 구성(18.4.11.C.01.)	guardduty-eks-protection-runtime-enabled	이 제어는 자동 에이전트 관리를 사용한 GuardDuty EKS 런타임 모니터링이 활성화되어 있는지 확인합니다. Amazon GuardDuty의 EKS 보호는 AWS 환경 내에서 Amazon EKS 클러스터를 보호하는 데 도움이 되는 위협 탐지 범위를 제공합니다. EKS 런타임 모니터링은 운영 체제 수준 이벤트를 사용하여 Amazon EKS 클러스터 내의 Amazon EKS 노드 및 컨테이너에서 잠재적 위협을 탐지하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3857	네트워크 보안, 침입 탐지 및 방지, IDS/IPS 구성(18.4.11.C.01.)	guardduty-lambda-protection-enabled	이 제어는 GuardDuty Lambda 보호가 활성화되어 있는지 확인합니다. GuardDuty Lambda 보호는 AWS Lambda 함수가 호출될 때 잠재적 보안 위협을 식별하는 데 도움이 됩니다. Lambda 보호를 활성화하면 GuardDuty는 AWS 계정의 Lambda 함수와 연결된 Lambda 네트워크 활동 로그 모니터링을 시작합니다. Lambda 함수가 호출되고 GuardDuty가 Lambda 함수에서 잠재적 악성 코드가 있음을 나타내는 의심스러운 네트워크 트래픽을 식별하면 조사 결과를 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3857	네트워크 보안, 침입 탐지 및 방지, IDS/IPS 구성(18.4.11.C.01.)	guardduty-s3-protection-enabled	이 제어는 GuardDuty S3 보호가 활성화되어 있는지 확인합니다. S3 보호를 사용하면 GuardDuty가 객체 수준 API 작업을 모니터링하여 Amazon S3 버킷 내의 데이터에 대한 잠재적 보안 위험을 식별할 수 있습니다. GuardDuty는 AWS CloudTrail 관리 이벤트 및 CloudTrail S3 데이터 이벤트를 분석하여 S3 리소스에 대한 위협을 모니터링합니다.
3875	네트워크 보안, 침입 탐지 및 방지, 이벤트 관리 및 상관관계(18.4.12.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3875	네트워크 보안, 침입 탐지 및 방지, 이벤트 관리 및 상관관계(18.4.12.C.01.)	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management(IAM) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4333	데이터 관리, 콘텐츠 필터링, 콘텐츠 검증 (20.3.7.C.02.)	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치고 보안을 손상시키거나 리소스를 과도하게 소비할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4333	데이터 관리, 콘텐츠 필터링, 콘텐츠 검증 (20.3.7.C.02.)	api-gw-associated-with-waf	이 제어는 API Gateway 단계에서 AWS WAF 웹 액세스 제어 목록(ACL)을 사용하는지 확인합니다. AWS WAF 리전 웹 ACL이 REST API Gateway 단계에 연결되지 않은 경우이 제어가 실패합니다. AWS WAF는 웹 애플리케이션과 APIs를 공격으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 이를 통해 사용자 정의 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 집합인 ACL을 구성할 수 있습니다. API Gateway 단계가 AWS WAF 웹 ACL과 연결되어 있는지 확인하여 악의적인 공격으로부터 보호합니다. API Gateway가 WAF가 활성화된 CloudFront 배포의 오리진인 경우 예외를 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4441	데이터 관리, 데이터베이스, 데이터베이스 파일(20.4.4.C.02.)	elasticsearch-encrypted-at-rest	이 제어는 Elasticsearch 도메인encryption-at-rest 구성이 활성화되어 있는지 확인합니다. 유휴 시 암호화가 활성화되지 않은 경우, 이 확인이 실패합니다. 민감한 데이터에 대한 보안 계층을 추가하려면 저장 시 암호화되도록 Elasticsearch Service 도메인을 구성해야 합니다. 저장 데이터의 암호화를 구성하면 AWS KMS는 암호화 키를 저장하고 관리합니다. 암호화를 수행하기 위해 AWS KMS는 256비트 키(AES-256)와 함께 고급 암호화 표준 알고리즘을 사용합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4441	데이터 관리, 데이터베이스, 데이터베이스 파일(20.4.4.C.02.)	opensearch-encrypted-at-rest	이 제어는 OpenSearch 도메인에 저장 시 암호화 구성이 활성화되어 있는지 확인합니다. 유휴 시 암호화가 활성화되지 않은 경우, 이 확인이 실패합니다. 중요한 데이터에 대한 보안 계층을 추가하려면 OpenSearch Service 도메인이 저장 시 암호화되도록 구성해야 합니다. 저장 데이터의 암호화를 구성하면 AWS KMS는 암호화 키를 저장하고 관리합니다. 암호화를 수행하기 위해 AWS KMS는 256비트 키(AES-256)와 함께 고급 암호화 표준 알고리즘을 사용합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4441	데이터 관리, 데이터베이스, 데이터베이스 파일(20.4.4.C.02.)	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
4441	데이터 관리, 데이터베이스, 데이터베이스 파일(20.4.4.C.02.)	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4441	데이터 관리, 데이터베이스, 데이터베이스 파일(20.4.4.C.02.)	rds-snapshots-public-prohibited	Amazon Relational Database Service(RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
4441	데이터 관리, 데이터베이스, 데이터베이스 파일(20.4.4.C.02.)	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4441	데이터 관리, 데이터베이스, 데이터베이스 파일(20.4.4.C.02.)	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙은 clusterDbEncrypted를 TRUE로 설정하고 loggingEnabled를 TRUE로 설정합니다.
4445	데이터 관리, 데이터베이스, 책임(20.4.5.C.02.)	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4445	데이터 관리, 데이터베이스, 책임(20.4.5.C.02.)	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙은 clusterDbEncrypted를 TRUE로 설정하고 loggingEnabled를 TRUE로 설정합니다.
4829	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 시스템 가용성(22.1.23.C.01.)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4829	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 시스템 가용성 (22.1.23.C.01.)	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4829	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 시스템 가용성 (22.1.23.C.01.)	rds-cluster-multi-az-enabled	Amazon Aurora는 단일 AWS 리전의 여러 가용 영역에 걸쳐 DB 클러스터에 데이터 사본을 저장합니다. Aurora는 DB 클러스터의 인스턴스가 여러 가용성 영역에 걸쳐 있는지 여부에 관계없이 이러한 복사본을 저장합니다. 기본 DB 인스턴스에 데이터가 기록되면 Aurora에서 가용 영역의 데이터를 클러스터 볼륨과 연결된 6개의 스토리지 노드에 동기적으로 복제합니다. 이 방법은 데이터 중복을 제공하고, I/O 중지를 없애고, 시스템 백업 중에 지연 시간 스파이크를 최소화합니다. DB 인스턴스를 고가용성으로 실행하면 계획된 시스템 유지 관리 중 가용성을 향상시킬 수 있으며, 데이터베이스에서 오류 및 가용 영역 중단이 일어나는 것을 방지할 수 있습니다. 이 규칙은 Amazon RDS에서 관리하는 Amazon Aurora 클러스터에서

제어 ID	제어 설명	AWS 구성 규칙	지침
			다중 AZ 복제가 활성화되어 있는지 확인합니다. 사전 프로덕션 환경에는 예외가 적용됩니다.
4829	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 시스템 가용성 (22.1.23.C.01.)	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다. 사전 프로덕션 환경에는 예외가 적용됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4838	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.03.)	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
4838	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.03.)	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4838	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.03.)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙은 ignorePublicAcls를 TRUE로, blockPublicPolicy를 TRUE로, blockPublicAcls를 TRUE로, restrictPublicBuckets를 TRUE로 설정합니다.
4838	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.03.)	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4838	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.03.)	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	elasticsearch-encrypted-at-rest	이 제어는 Elasticsearch 도메인encryption-at-rest 구성이 활성화되어 있는지 확인합니다. 유휴 시 암호화가 활성화되지 않은 경우, 이 확인이 실패합니다. 민감한 데이터에 대한 보안 계층을 추가하려면 저장 시 암호화되도록 Elasticsearch Service 도메인을 구성해야 합니다. 저장 데이터의 암호화를 구성하면 AWS KMS는 암호화 키를 저장하고 관리합니다. 암호화를 수행하기 위해 AWS KMS는 256비트 키(AES-256)와 함께 고급 암호화 표준 알고리즘을 사용합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	elasticsearch-node-to-node-encryption-check	이 제어는 Elasticsearch 도메인에 노드 간 암호화를 활성화하고 있는지 확인합니다. 도메인에서 노드 간 암호화를 비활성화하면 이 제어가 실패합니다. HTTPS(TLS)를 사용하면 잠재적인 공격자가 중간자 또는 유사한 공격을 통해 네트워크 트래픽을 도청하거나 조작하는 것을 방지할 수 있습니다. HTTPS(TLS)를 통한 암호화된 연결만 허용되어야 합니다. Elasticsearch 도메인의 노드 간 암호화를 활성화하면 클러스터 내 통신이 전송 중 암호화됩니다.
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	opensearch-encrypted-at-rest	이 제어는 OpenSearch 도메인에 저장 시 암호화 구성이 활성화되어 있는지 확인합니다. 유휴 시 암호화가 활성화되지 않은 경우, 이 확인이 실패합니다. 중요한 데이터에 대한 보안 계층을 추가하려면 OpenSearch Service 도메인이 저장 시 암호화되도록 구성해야 합니다. 저장 데이터의 암호화를 구성하면 AWS KMS는 암호화 키를 저장하고 관리합니다. 암호화를 수행하기 위해 AWS KMS는 256비트 키(AES-256)와 함께 고급 암호화 표준 알고리즘을 사용합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	opensearch-node-to-node-encryption-check	이 제어는 OpenSearch 도메인에 노드 간 암호화가 활성화되어 있는지 확인합니다. 도메인에서 노드 간 암호화를 비활성화하면 이 제어가 실패합니다. HTTPS(TLS)를 사용하면 잠재적인 공격자가 중간자 또는 유사한 공격을 통해 네트워크 트래픽을 도청하거나 조작하는 것을 방지할 수 있습니다. HTTPS(TLS)를 통한 암호화된 연결만 허용되어야 합니다. OpenSearch 도메인에 대해 노드 간 암호화를 활성화하면 클러스터 내 통신이 전송 중 암호화됩니다.
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙은 clusterDbEncrypted를 TRUE로 설정하고 loggingEnabled를 TRUE로 설정합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하려면 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하려면 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	secretsmanager-using-cmk	저장 데이터를 보호하려면 AWS Secrets Manager 보안 암호에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
4839	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 무단 액세스(22.1.24.C.04)	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다. 주제에 게시된 메시지에 민감한 데이터가 포함되지 않은 경우 예외를 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4849	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 백업, 복구 아카이빙 및 데이터 보존 (22.1.26.C.01.)	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
4849	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 백업, 복구 아카이빙 및 데이터 보존 (22.1.26.C.01.)	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 보정 복구 솔루션이 구성된 경우 공제를 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4849	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 백업, 복구 아카이빙 및 데이터 보존 (22.1.26.C.01.)	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
4849	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 백업, 복구 아카이빙 및 데이터 보존 (22.1.26.C.01.)	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 보정 복구 솔루션이 구성된 경우 공제를 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4849	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 백업, 복구 아카이빙 및 데이터 보존 (22.1.26.C.01.)	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 보정 복구 솔루션이 구성된 경우 공제를 사용할 수 있습니다.
4849	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 백업, 복구 아카이빙 및 데이터 보존 (22.1.26.C.01.)	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4849	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 백업, 복구 아카이빙 및 데이터 보존 (22.1.26.C.01.)	rds-cluster-deletion-protection-enabled	Amazon RDS 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 삭제 방지 기능을 사용하여 RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
4849	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 백업, 복구 아카이빙 및 데이터 보존 (22.1.26.C.01.)	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 보정 복구 솔루션이 구성된 경우 공제를 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4849	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 백업, 복구 아카이빙 및 데이터 보존 (22.1.26.C.01.)	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
4849	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 백업, 복구 아카이빙 및 데이터 보존 (22.1.26.C.01.)	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4849	엔터프라이즈 시스템 보안, 클라우드 컴퓨팅, 백업, 복구 아카이빙 및 데이터 보존 (22.1.26.C.01.)	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다. 객체의 단일 변형만 생성되거나 보정 복구 솔루션이 구성된 경우 면제를 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6843	액세스 제어 및 암호, 권한 있는 액세스 관리, 최소 권한의 원칙 (16.4.31.C.02.)	mfa-enabled-for-iam-console-access	MFA는 사용자가 AWS 웹 사이트 또는 서비스에 액세스할 때 일반 로그인 자격 증명 외에도 AWS 지원 MFA 메커니즘에서 고유한 인증을 제공하도록 요구하여 보안을 강화합니다. 지원되는 메커니즘에는 U2F 보안 키, 가상 또는 하드웨어 MFA 디바이스, SMS 기반 코드가 포함됩니다. 이 규칙은 콘솔 암호를 사용하는 모든 AWS Identity and Access Management AWS Multi-Factor Authentication (MFA))이 활성화되어 있는지 확인합니다. MFA가 활성화된 경우 규칙은 규정을 준수합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6843	액세스 제어 및 암호, 권한 있는 액세스 관리, 최소 권한의 원칙 (16.4.31.C.02.)	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 AWS 계정에서 가장 권한이 있는 사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 AWS 계정의 인시던트를 줄일 수 있습니다.
6852	액세스 제어 및 암호, 권한 있는 액세스 관리, 권한 있는 액세스 자격 증명의 일시 중지 및 취소(16.4.33.C.01.)	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙은 maxCredentialUsageAge를 30일로 설정합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6860	액세스 제어 및 암호, 권한 있는 액세스 관리, 모니터링 및 검토 (16.4.35.C.02.)	cloud-trail-cloud-watch-logs-enabled	추적 로그를 모니터링하고 특정 활동이 발생할 때 알림을 받도록 CloudWatch Logs로 CloudTrailCloudTrail을 구성해야 합니다. 이 규칙은 AWS CloudTrail 추적이 Amazon CloudWatch logs 로그로 로그를 전송하도록 구성되어 있는지 확인합니다.
6860	액세스 제어 및 암호, 권한 있는 액세스 관리, 모니터링 및 검토 (16.4.35.C.02.)	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6861	액세스 제어 및 암호, 권한 있는 액세스 관리, 모니터링 및 검토 (16.4.35.C.03.)	cloudtrail-security-trail-enabled	이 규칙은 여러 설정의 활성화를 확인하여 AWS CloudTrail에 AWS 권장되는 보안 모범 사례를 사용하는 데 도움이 됩니다. 여기에는 여러 리전에서 로그 암호화, 로그 검증 및 Enable AWS CloudTrail 사용이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6953	액세스 제어 및 암호, 다중 인증, 시스템 아키텍처 및 보안 제어 (16.7.34.C.02.)	mfa-enabled-for-iam-console-access	MFA는 사용자가 AWS 웹 사이트 또는 서비스에 액세스할 때 일반 로그인 자격 증명 외에도 AWS 지원 MFA 메커니즘에서 고유한 인증을 제공하도록 요구하여 보안을 강화합니다. 지원되는 메커니즘에는 U2F 보안 키, 가상 또는 하드웨어 MFA 디바이스, SMS 기반 코드가 포함됩니다. 이 규칙은 콘솔 암호를 사용하는 모든 AWS Identity and Access Management AWS Multi-Factor Authentication (MFA))이 활성화되어 있는지 확인합니다. MFA가 활성화된 경우 규칙은 규정을 준수합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6953	액세스 제어 및 암호, 다중 인증, 시스템 아키텍처 및 보안 제어 (16.7.34.C.02.)	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 AWS 계정에서 가장 권한이 있는 사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 AWS 계정의 인시던트를 줄일 수 있습니다.
7436	퍼블릭 클라우드 보안, 자격 증명 관리 및 액세스 제어, 사용자 이름 및 암호(23.3.19.C.01.)	iam-user-mfa-enabled	이 규칙을 활성화하여 AWS 클라우드의 리소스에 대한 액세스를 제한합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
7436	퍼블릭 클라우드 보안, 자격 증명 관리 및 액세스 제어, 사용자 이름 및 암호(23.3.19.C.01.)	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7436	퍼블릭 클라우드 보안, 자격 증명 관리 및 액세스 제어, 사용자 이름 및 암호(23.3.19.C.01.)	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 AWS 계정에서 가장 권한이 있는 사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 AWS 계정의 인시던트를 줄일 수 있습니다.
7436	퍼블릭 클라우드 보안, 자격 증명 관리 및 액세스 제어, 사용자 이름 및 암호(23.3.19.C.01.)	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 AWS 계정에서 가장 권한이 있는 사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 AWS 계정의 인시던트를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7437	퍼블릭 클라우드 보안, 자격 증명 관리 및 액세스 제어, 사용자 이름 및 암호(23.3.19.C.01.)	iam-user-mfa-enabled	이 규칙을 활성화하여 AWS 클라우드의 리소스에 대한 액세스를 제한합니다. 이 규칙은 모든 IAM 사용자에 대해 다중 인증(MFA)을 활성화합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
7437	퍼블릭 클라우드 보안, 자격 증명 관리 및 액세스 제어, 사용자 이름 및 암호(23.3.19.C.01.)	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. IAM 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7437	퍼블릭 클라우드 보안, 자격 증명 관리 및 액세스 제어, 사용자 이름 및 암호(23.3.19.C.01.)	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 AWS 계정에서 가장 권한이 있는 사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 AWS 계정의 인시던트를 줄일 수 있습니다.
7437	퍼블릭 클라우드 보안, 자격 증명 관리 및 액세스 제어, 사용자 이름 및 암호(23.3.19.C.01.)	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 AWS 계정에서 가장 권한이 있는 사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 AWS 계정의 인시던트를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	api-gw-associated-with-waf	이 제어는 API Gateway 단계에서 AWS WAF 웹 액세스 제어 목록(ACL)을 사용하는지 확인합니다. AWS WAF 리전 웹 ACL이 REST API Gateway 단계에 연결되지 않은 경우이 제어가 실패합니다. AWS WAF는 웹 애플리케이션과 APIs를 공격으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 이를 통해 사용자 정의 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 집합인 ACL을 구성할 수 있습니다. API Gateway 단계가 AWS WAF 웹 ACL과 연결되어 있는지 확인하여 악의적인 공격으로부터 보호합니다. API Gateway가 WAF가 활성화된 CloudFront 배포의 오리진인 경우 예외를 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	elasticsearch-in-vpc-only	이 제어는 Elasticsearch 도메인이 VPC에 있는지 확인합니다. 퍼블릭 액세스를 확인하기 위해 VPC 서브넷 라우팅 구성을 평가하지 않습니다. Elasticsearch 도메인이 퍼블릭 서브넷에 연결되어 있지 않은지 확인해야 합니다. VPC 내에 배포된 Elasticsearch 도메인은 퍼블릭 인터넷을 통과할 필요 없이 프라이빗 AWS 네트워크를 통해 VPC 리소스와 통신할 수 있습니다. 이 구성은 전송 중 데이터에 대한 액세스를 제한하여 보안 상태를 강화합니다. VPCs 네트워크 ACL 및 보안 그룹을 포함하여 Elasticsearch 도메인에 대한 액세스를 보호하기 위한 여러 네트워크 제어를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	opensearch-in-vpc-only	이 제어는 OpenSearch 도메인이 VPC에 있는지 확인합니다. 퍼블릭 액세스를 확인하기 위해 VPC 서브넷 라우팅 구성을 평가하지 않습니다. OpenSearch 도메인이 퍼블릭 서브넷에 연결되어 있지 않은지 확인해야 합니다. VPC 내에 배포된 OpenSearch 도메인은 퍼블릭 인터넷을 통과할 필요 없이 프라이빗 AWS 네트워크를 통해 VPC 리소스와 통신할 수 있습니다. 이 구성은 전송 중 데이터에 대한 액세스를 제한하여 보안 상태를 강화합니다. VPC는 네트워크 ACL 및 보안 그룹을 포함하여 OpenSearch 도메인에 대한 액세스를 보호하기 위한 다양한 네트워크 제어를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	rds-instance-public-access-check	Amazon Relational Database Service(RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙은 ignorePublicAcls를 TRUE로, blockPublicPolicy를 TRUE로, blockPublicAcls를 TRUE로, restrictPublicBuckets를 TRUE로 설정합니다.
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북이 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 수신 및 송신 네트워크 트래픽의 상태 저장 필터링을 제공하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7466	퍼블릭 클라우드 보안, 퍼블릭 클라우드의 데이터 보호, 데이터 접근성(23.4.10.C.01.)	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
7496	퍼블릭 클라우드의 퍼블릭 클라우드 보안, 로깅 및 알림, 로깅 요구 사항(23.5.11.C.01.)	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7496	퍼블릭 클라우드의 퍼블릭 클라우드 보안, 로깅 및 알림, 로깅 요구 사항(23.5.11.C.01.)	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7496	퍼블릭 클라우드의 퍼블릭 클라우드 보안, 로깅 및 알림, 로깅 요구 사항(23.5.11.C.01.)	cloudfront-accesslogs-enabled	이 제어는 CloudFront 배포에서 서버 액세스 로깅이 활성화되었는지 여부를 확인합니다. 배포에 대한 액세스 로깅이 활성화되지 않은 경우, 제어가 실패합니다. CloudFront 액세스 로그는 CloudFront가 수신하는 모든 사용자 요청에 대한 세부 정보를 제공합니다. 각 로그에는 요청이 수신된 날짜 및 시간, 요청한 뷰어의 IP 주소, 요청 소스, 뷰어의 요청 포트 번호 등의 정보가 포함됩니다. 이러한 로그는 보안 및 액세스 감사, 포렌식 조사와 같은 목적에 유용합니다. us-east-1 리전에서는 이 규칙을 반드시 적용해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7496	퍼블릭 클라우드의 퍼블릭 클라우드 보안, 로깅 및 알림, 로깅 요구 사항(23.5.11.C.01.)	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출한 사용자 및 AWS 계정, 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
7496	퍼블릭 클라우드의 퍼블릭 클라우드 보안, 로깅 및 알림, 로깅 요구 사항(23.5.11.C.01.)	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
7496	퍼블릭 클라우드의 퍼블릭 클라우드 보안, 로깅 및 알림, 로깅 요구 사항(23.5.11.C.01.)	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.
7496	퍼블릭 클라우드의 퍼블릭 클라우드 보안, 로깅 및 알림, 로깅 요구 사항(23.5.11.C.01.)	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7496	퍼블릭 클라우드의 퍼블릭 클라우드 보안, 로깅 및 알림, 로깅 요구 사항(23.5.11.C.01.)	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보, 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.

템플릿

템플릿은 GitHub: NZISM 운영 모범 사례에서 확인할 수 있습니다.

PCI DSS 3.2.1 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Payment Card Industry Data Security Standard(PCI DSS) 3.2.1과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 AWS Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 PCI DSS 제어와 관련이 있습니다. PCI DSS 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	alb-desync-mode-check	HTTP 비동기 취약성으로부터 애플리케이션을 보호하려면 애플리케이션 로드 밸런서에서 HTTP 비동기화 완화 모드를 활성화해야 합니다. HTTP 비동기화 문제로 인해 요청 밀수가 발생하고 애플리케이션이 요청 대기열 또는 캐시 중독에 취약해질 수 있습니다. 비동기화 완화 모드에는 모니터링, 방어 및 가장 엄격 모드가 있습니다. 기본 모드는 방어 모드입니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네

제어 ID	제어 설명	AWS 구성 규칙	지침
			트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	netfw-stateless-rule-group-not-empty	AWS Network Firewall 규칙 그룹에는 방화벽이 VPC에서 트래픽을 처리하는 방법을 정의하는 규칙이 포함되어 있습니다. 방화벽 정책에 있는 빈 상태 비저장 규칙 그룹은 트래픽을 처리하지 않습니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않도록 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3	카드 소지자 데이터 환경의 인터넷과 모든 시스템 구성 요소 간에 직접 퍼블릭 액세스를 금지합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	netfw-policy-rule-group-associated	AWS Network Firewall 정책은 방화벽이 Amazon VPC에서 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하여 패킷과 트래픽 흐름을 필터링하고 기본 트래픽 처리를 정의합니다.
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	netfw-stateless-rule-group-not-empty	AWS Network Firewall 규칙 그룹에는 방화벽이 VPC에서 트래픽을 처리하는 방법을 정의하는 규칙이 포함되어 있습니다. 방화벽 정책에 있는 빈 상태 비저장 규칙 그룹은 트래픽을 처리하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.6	데이터베이스 등 카드 소지자 데이터가 저장된 시스템 구성 요소를 내부 네트워크 영역에 DMZ 및 신뢰할 수 없는 기타 네트워크와 분리하여 배치합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1	네트워크에 시스템을 설치하기 전에 항상 공급업체에서 제공한 기본값을 변경하고 불필요한 기본 계정을 제거하거나 비활성화합니다. 이는 운영 체제, 보안 서비스를 제공하는 소프트웨어, 애플리케이션 및 시스템 계정, 판매 시점 정보 관리(POS) 단말기, 결제 애플리케이션, 간이 망 관리 프로토콜(SNMP) 커뮤니티 문자열 등에서 사용되는 암호를 포함하되 이에 국한되지 않는 모든 기본 암호에 적용됩니다.	rds-cluster-default-admin-check	기본 사용자 이름은 공개적으로 알려져 있으므로 기본 사용자 이름을 변경하면 Amazon Relational Database Service(RDS) 데이터베이스 클러스터의 공격 표면을 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1	네트워크에 시스템을 설치하기 전에 항상 공급업체에서 제공한 기본값을 변경하고 불필요한 기본 계정을 제거하거나 비활성화합니다. 이는 운영 체제, 보안 서비스를 제공하는 소프트웨어, 애플리케이션 및 시스템 계정, 판매 시점 정보 관리(POS) 단말기, 결제 애플리케이션, 간이 망 관리 프로토콜(SNMP) 커뮤니티 문자열 등에서 사용되는 암호를 포함하되 이에 국한되지 않는 모든 기본 암호에 적용됩니다.	rds-instance-default-admin-check	기본 사용자 이름은 공개적으로 알려져 있으므로 기본 사용자 이름을 변경하면 Amazon Relational Database Service(RDS) 데이터베이스 클러스터의 공격 표면을 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1	네트워크에 시스템을 설치하기 전에 항상 공급업체에서 제공한 기본값을 변경하고 불필요한 기본 계정을 제거하거나 비활성화합니다. 이는 운영 체제, 보안 서비스를 제공하는 소프트웨어, 애플리케이션 및 시스템 계정, 판매 시점 정보 관리(POS) 단말기, 결제 애플리케이션, 간이 망 관리 프로토콜(SNMP) 커뮤니티 문자열 등에서 사용되는 암호를 포함하되 이에 국한되지 않는 모든 기본 암호에 적용됩니다.	redshift-default-admin-check	기본 사용자 이름은 공개적으로 알려져 있으므로 기본 사용자 이름을 변경하면 Amazon Redshift 클러스터의 공격 표면을 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1	네트워크에 시스템을 설치하기 전에 항상 공급업체에서 제공한 기본값을 변경하고 불필요한 기본 계정을 제거하거나 비활성화합니다. 이는 운영 체제, 보안 서비스를 제공하는 소프트웨어, 애플리케이션 및 시스템 계정, 판매 시점 정보 관리(POS) 단말기, 결제 애플리케이션, 간이 망 관리 프로토콜(SNMP) 커뮤니티 문자열 등에서 사용되는 암호를 포함하되 이에 국한되지 않는 모든 기본 암호에 적용됩니다.	redshift-default-db-name-check	기본 이름은 공개적으로 알려져 있으므로 구성 시 변경해야 합니다. Amazon Redshift 클러스터의 기본 데이터베이스 이름을 변경하면 Redshift 클러스터의 공격 표면을 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1	네트워크에 시스템을 설치하기 전에 항상 공급업체에서 제공한 기본값을 변경하고 불필요한 기본 계정을 제거하거나 비활성화합니다. 이는 운영 체제, 보안 서비스를 제공하는 소프트웨어, 애플리케이션 및 시스템 계정, 판매 시점 정보 관리(POS) 단말기, 결제 애플리케이션, 간이 망 관리 프로토콜(SNMP) 커뮤니티 문자열 등에서 사용되는 암호를 포함하되 이에 국한되지 않는 모든 기본 암호에 적용됩니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.1	네트워크에 시스템을 설치하기 전에 항상 공급업체에서 제공한 기본값을 변경하고 불필요한 기본 계정을 제거하거나 비활성화합니다. 이는 운영 체제, 보안 서비스를 제공하는 소프트웨어, 애플리케이션 및 시스템 계정, 판매 시점 정보 관리(POS) 단말기, 결제 애플리케이션, 간이 망 관리 프로토콜(SNMP) 커뮤니티 문자열 등에서 사용되는 암호를 포함하되 이에 국한되지 않는 모든 기본 암호에 적용됩니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하기 위해 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	ec2-instance-multiple-eni-check	이 규칙은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 ENI가 여러 개 있는지 확인합니다. ENI가 여러 개 있으면 이중 홈 인스턴스, 즉 서브넷이 여러 개 있는 인스턴스가 발생할 수 있습니다. 이로 인해 네트워크 보안이 복잡해지고 의도하지 않은 네트워크 경로와 액세스가 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	ec2-security-group-attached-to-eni-periodic	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 직무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2	모든 시스템 구성 요소에 대한 구성 표준을 개발합니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다. 업계에서 인정하는 시스템 강화 표준의 출처에는 다음이 포함되며 이에 국한되지는 않습니다. • Center for Internet Security(CIS) • International Organization for Standardization(ISO) • SysAdmin Audit Network Security(SANS) Institute • National Institute of Standards Technology(NIST)	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화하세요.	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.2	서비스, 프로토콜, 데몬 등은 시스템이 기능하는 데 필요한 것만 활성화합니다.	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.3	안전하지 않은 것으로 간주되는 필수 서비스, 프로토콜 또는 데몬에 대해 추가 보안 기능을 구현하세요.	alb-desync-mode-check	HTTP 비동기 취약성으로부터 애플리케이션을 보호하려면 애플리케이션 로드 밸런서에서 HTTP 비동기화 완화 모드를 활성화해야 합니다. HTTP 비동기화 문제로 인해 요청 밀수가 발생하고 애플리케이션이 요청 대기열 또는 캐시 중독에 취약해질 수 있습니다. 비동기화 완화 모드에는 모니터링, 방어 및 가장 엄격 모드가 있습니다. 기본 모드는 방어 모드입니다.
2.3	강력한 암호화를 사용하여 콘솔이 아닌 모든 관리 액세스를 암호화합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.3	강력한 암호화를 사용하여 콘솔이 아닌 모든 관리 액세스를 암호화합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
2.3	강력한 암호화를 사용하여 콘솔이 아닌 모든 관리 액세스를 암호화합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.3	강력한 암호화를 사용하여 콘솔이 아닌 모든 관리 액세스를 암호화합니다.	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.3	강력한 암호화를 사용하여 콘솔이 아닌 모든 관리 액세스를 암호화합니다.	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.4	PCI DSS 범위에 있는 시스템 구성 요소의 인벤토리를 유지 관리합니다.	ec2-security-group-attached-to-eni-periodic	이 규칙은 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 ENI에 연결되도록 합니다. 이 규칙은 인벤토리에서 사용하지 않는 보안 그룹을 모니터링하고 환경을 관리하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.4	PCI DSS 범위에 있는 시스템 구성 요소의 인벤토리를 유지 관리합니다.	eip-attached	이 규칙은 Amazon Virtual Private Cloud(VPC)에 할당된 탄력적 IP가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스에 연결되도록 합니다. 이 규칙은 사용자 환경에서 사용되지 않는 EIP를 모니터링하는 데 도움이 됩니다.
2.4	PCI DSS 범위에 있는 시스템 구성 요소의 인벤토리를 유지 관리합니다.	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.4	PCI DSS 범위에 있는 시스템 구성 요소의 인벤토리를 유지 관리합니다.	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1	모든 카드 소지자 데이터(CHD) 스토리지에 대해 최소한 다음을 포함하는 데이터 보존 및 폐기 정책, 절차 및 프로세스를 구현하여 카드 소지자 데이터 스토리지를 최소화합니다. • 데이터 스토리지 용량 및 보존 시간을 법률, 규제 및/또는 비즈니스 요구 사항에 필요한 수준으로 제한 • 카드 소지자 데이터에 대한 특정 보존 요구 사항 • 더 이상 필요하지 않을 경우 데이터를 안전하게 삭제하는 프로세스 • 정의된 보존 기간을 초과하는 저장된 카드 소지자 데이터를 식별하여 안전하게 삭제하기 위한 분기별 프로세스	s3-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1	모든 카드 소지자 데이터(CHD) 스토리지에 대해 최소한 다음을 포함하는 데이터 보존 및 폐기 정책, 절차 및 프로세스를 구현하여 카드 소지자 데이터 스토리지를 최소화합니다. • 데이터 스토리지 용량 및 보존 시간을 법률, 규제 및/또는 비즈니스 요구 사항에 필요한 수준으로 제한 • 카드 소지자 데이터에 대한 특정 보존 요구 사항 • 더 이상 필요하지 않을 경우 데이터를 안전하게 삭제하는 프로세스 • 정의된 보존 기간을 초과하는 저장된 카드 소지자 데이터를 식별하여 안전하게 삭제하기 위한 분기별 프로세스	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1	모든 카드 소지자 데이터(CHD) 스토리지에 대해 최소한 다음을 포함하는 데이터 보존 및 폐기 정책, 절차 및 프로세스를 구현하여 카드 소지자 데이터 스토리지를 최소화합니다. • 데이터 스토리지 용량 및 보존 시간을 법률, 규제 및/또는 비즈니스 요구 사항에 필요한 수준으로 제한 • 카드 소지자 데이터에 대한 특정 보존 요구 사항 • 더 이상 필요하지 않을 경우 데이터를 안전하게 삭제하는 프로세스 • 정의된 보존 기간을 초과하는 저장된 카드 소지자 데이터를 식별하여 안전하게 삭제하기 위한 분기별 프로세스	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1	모든 카드 소지자 데이터(CHD) 스토리지에 대해 최소한 다음을 포함하는 데이터 보존 및 폐기 정책, 절차 및 프로세스를 구현하여 카드 소지자 데이터 스토리지를 최소화합니다. • 데이터 스토리지 용량 및 보존 시간을 법률, 규제 및/또는 비즈니스 요구 사항에 필요한 수준으로 제한 • 카드 소지자 데이터에 대한 특정 보존 요구 사항 • 더 이상 필요하지 않을 경우 데이터를 안전하게 삭제하는 프로세스 • 정의된 보존 기간을 초과하는 저장된 카드 소지자 데이터를 식별하여 안전하게 삭제하기 위한 분기별 프로세스	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.4	다음 방법 중 하나를 사용하여 저장된 곳(휴대용 디지털 미디어, 백업 미디어 및 로그 포함)에서 PAN을 읽을 수 없게 만듭니다. • 강력한 암호화를 기반으로 하는 단방향 해시(해시는 전체 PAN의 것이어야 함) • 잘라내기(해시는 PAN의 잘린 부분을 대체하는 데 사용할 수 없음) • 인덱스 토큰 및 패드(패드는 안전하게 저장해야 함) • 강력한 암호화 및 관련 키 관리 프로세스 및 절차 참고: 악의적인 개인이 PAN의 잘린 버전과 해시된 버전 모두에 액세스할 수 있는 경우 원본 PAN 데이터를 재구성하는 것은 비교적 간단한 작업입니다. 엔티티 환경에 동일한 PAN의 해시된 버전과 잘린 버전이 있는 경우 원래 PAN을 재구성하기 위해 해시된 버전과 잘린 버전을 상호 연관시키지 않도록 추가 제어 기능을 마련해야 합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.2	암호화 키에 대한 액세스를 필요한 최소 수의 관리자로 제한하세요.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.2	암호화 키에 대한 액세스를 필요한 최소 수의 관리자로 제한하세요.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.3	카드 소지자 데이터를 암호화/복호화하는 데 사용되는 비밀 키와 개인 키를 항상 다음 형식 중 하나(또는 그 이상)로 저장합니다. • 최소한 데이터 암호화 키만큼 강력한 키 암호화 키로 암호화되고 데이터 암호화 키와는 별도로 저장 • 안전한 암호화 장치(예: 하드웨어(호스트) 보안 모듈(HSM) 또는 PTS 승인 상호 작용 장치 내에 보관) • 업계에서 인정하는 방법에 따라 최소 두 개의 전체 길이 키 구성 요소 또는 키 공유로 사용 (참고: 공개 키를 이러한 형태 중 하나로 저장할 필요는 없습니다.)	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.3	카드 소지자 데이터를 암호화/복호화하는 데 사용되는 비밀 키와 개인 키를 항상 다음 형식 중 하나(또는 그 이상)로 저장합니다. • 최소한 데이터 암호화 키만큼 강력한 키 암호화 키로 암호화되고 데이터 암호화 키와는 별도로 저장 • 안전한 암호화 장치(예: 하드웨어(호스트) 보안 모듈(HSM) 또는 PTS 승인 상호 작용 장치 내에 보관) • 업계에서 인정하는 방법에 따라 최소 두 개의 전체 길이 키 구성 요소 또는 키 공유로 사용 (참고: 공개 키를 이러한 형태 중 하나로 저장할 필요는 없습니다.)	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.3	카드 소지자 데이터를 암호화/복호화하는 데 사용되는 비밀 키와 개인 키를 항상 다음 형식 중 하나(또는 그 이상)로 저장합니다. • 최소한 데이터 암호화 키만큼 강력한 키 암호화 키로 암호화되고 데이터 암호화 키와는 별도로 저장 • 안전한 암호화 장치(예: 하드웨어(호스트) 보안 모듈(HSM) 또는 PTS 승인 상호 작용 장치 내에 보관) • 업계에서 인정하는 방법에 따라 최소 두 개의 전체 길이 키 구성 요소 또는 키 공유로 사용 (참고: 공개 키를 이러한 형태 중 하나로 저장할 필요는 없습니다.)	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.4	관련 애플리케이션 공급업체 또는 키 소유자가 정의하고 업계 모범 사례 및 지침(예: NIST 특별 간행물 800-57)에 따라 암호화 기간이 종료된 후(예: 정의된 기간이 지난 후 및/또는 해당 키에서 일정량의 암호문이 생성된 후) 키에 대한 암호화 키 변경	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
3.6.5	키의 무결성이 약화된 경우(예: 일반 텍스트 키 구성 요소를 알고 있는 직원이 퇴사) 또는 키 손상이 의심되는 경우 필요하다고 판단되는 키의 폐기 또는 교체(예: 보관, 폐기 및/또는 취소) 참고: 사용 중지되거나 교체된 암호화 키를 유지해야 하는 경우 이러한 키를 안전하게 보관해야 합니다(예: 키 암호화 키 사용). 보관된 암호화 키는 암호 해독 및 확인 목적으로만 사용해야 합니다.	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.7	암호화 키의 무단 대체 방지	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	다음과 같은 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화 및 보안 프로토콜을 사용하여 민감한 카드 소지자 데이터를 보호합니다. • 신뢰할 수 있는 키와 인증서만 허용됩니다. • 사용 중인 프로토콜은 보안 버전 또는 구성만 지원합니다. • 암호화 강도는 사용 중인 암호화 방법에 적합합니다. 개방형 공용 네트워크의 예로는 다음이 포함되며 이에 국한되지 않습니다. • 인터넷 • 802.11 및 Bluetooth를 포함한 무선 기술 • 셀룰러 기술[예: 글로벌 이동 통신 시스템(GSM), 코드 분할 다중 액세스(CDMA) • 일반 패킷 라디오 서비스(GPRS)] • 위성 통신	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	다음과 같은 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화 및 보안 프로토콜을 사용하여 민감한 카드 소지자 데이터를 보호합니다. • 신뢰할 수 있는 키와 인증서만 허용됩니다. • 사용 중인 프로토콜은 보안 버전 또는 구성만 지원합니다. • 암호화 강도는 사용 중인 암호화 방법에 적합합니다. 개방형 공용 네트워크의 예로는 다음이 포함되며 이에 국한되지 않습니다. • 인터넷 • 802.11 및 Bluetooth를 포함한 무선 기술 • 셀룰러 기술[예: 글로벌 이동 통신 시스템(GSM), 코드 분할 다중 액세스(CDMA) • 일반 패킷 라디오 서비스(GPRS)] • 위성 통신	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	다음과 같은 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화 및 보안 프로토콜을 사용하여 민감한 카드 소지자 데이터를 보호합니다. • 신뢰할 수 있는 키와 인증서만 허용됩니다. • 사용 중인 프로토콜은 보안 버전 또는 구성만 지원합니다. • 암호화 강도는 사용 중인 암호화 방법에 적합합니다. 개방형 공용 네트워크의 예로는 다음이 포함되며 이에 국한되지 않습니다. • 인터넷 • 802.11 및 Bluetooth를 포함한 무선 기술 • 셀룰러 기술[예: 글로벌 이동 통신 시스템(GSM), 코드 분할 다중 액세스(CDMA) • 일반 패킷 라디오 서비스(GPRS)] • 위성 통신	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	다음과 같은 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화 및 보안 프로토콜을 사용하여 민감한 카드 소지자 데이터를 보호합니다. • 신뢰할 수 있는 키와 인증서만 허용됩니다. • 사용 중인 프로토콜은 보안 버전 또는 구성만 지원합니다. • 암호화 강도는 사용 중인 암호화 방법에 적합합니다. 개방형 공용 네트워크의 예로는 다음이 포함되며 이에 국한되지 않습니다. • 인터넷 • 802.11 및 Bluetooth를 포함한 무선 기술 • 셀룰러 기술[예: 글로벌 이동 통신 시스템(GSM), 코드 분할 다중 액세스(CDMA) • 일반 패킷 라디오 서비스(GPRS)] • 위성 통신	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	다음과 같은 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화 및 보안 프로토콜을 사용하여 민감한 카드 소지자 데이터를 보호합니다. • 신뢰할 수 있는 키와 인증서만 허용됩니다. • 사용 중인 프로토콜은 보안 버전 또는 구성만 지원합니다. • 암호화 강도는 사용 중인 암호화 방법에 적합합니다. 개방형 공용 네트워크의 예로는 다음이 포함되며 이에 국한되지 않습니다. • 인터넷 • 802.11 및 Bluetooth를 포함한 무선 기술 • 셀룰러 기술[예: 글로벌 이동 통신 시스템(GSM), 코드 분할 다중 액세스(CDMA) • 일반 패킷 라디오 서비스(GPRS)] • 위성 통신	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	다음과 같은 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화 및 보안 프로토콜을 사용하여 민감한 카드 소지자 데이터를 보호합니다. • 신뢰할 수 있는 키와 인증서만 허용됩니다. • 사용 중인 프로토콜은 보안 버전 또는 구성만 지원합니다. • 암호화 강도는 사용 중인 암호화 방법에 적합합니다. 개방형 공용 네트워크의 예로는 다음이 포함되며 이에 국한되지 않습니다. • 인터넷 • 802.11 및 Bluetooth를 포함한 무선 기술 • 셀룰러 기술[예: 글로벌 이동 통신 시스템(GSM), 코드 분할 다중 액세스(CDMA) • 일반 패킷 라디오 서비스(GPRS)] • 위성 통신	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	다음과 같은 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화 및 보안 프로토콜을 사용하여 민감한 카드 소지자 데이터를 보호합니다. • 신뢰할 수 있는 키와 인증서만 허용됩니다. • 사용 중인 프로토콜은 보안 버전 또는 구성만 지원합니다. • 암호화 강도는 사용 중인 암호화 방법에 적합합니다. 개방형 공용 네트워크의 예로는 다음이 포함되며 이에 국한되지 않습니다. • 인터넷 • 802.11 및 Bluetooth를 포함한 무선 기술 • 셀룰러 기술[예: 글로벌 이동 통신 시스템(GSM), 코드 분할 다중 액세스(CDMA) • 일반 패킷 라디오 서비스(GPRS)] • 위성 통신	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	다음과 같은 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화 및 보안 프로토콜을 사용하여 민감한 카드 소지자 데이터를 보호합니다. • 신뢰할 수 있는 키와 인증서만 허용됩니다. • 사용 중인 프로토콜은 보안 버전 또는 구성만 지원합니다. • 암호화 강도는 사용 중인 암호화 방법에 적합합니다. 개방형 공용 네트워크의 예로는 다음이 포함되며 이에 국한되지 않습니다. • 인터넷 • 802.11 및 Bluetooth를 포함한 무선 기술 • 셀룰러 기술[예: 글로벌 이동 통신 시스템(GSM), 코드 분할 다중 액세스(CDMA) • 일반 패킷 라디오 서비스(GPRS)] • 위성 통신	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	다음과 같은 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화 및 보안 프로토콜을 사용하여 민감한 카드 소지자 데이터를 보호합니다. • 신뢰할 수 있는 키와 인증서만 허용됩니다. • 사용 중인 프로토콜은 보안 버전 또는 구성만 지원합니다. • 암호화 강도는 사용 중인 암호화 방법에 적합합니다. 개방형 공용 네트워크의 예로는 다음이 포함되며 이에 국한되지 않습니다. • 인터넷 • 802.11 및 Bluetooth를 포함한 무선 기술 • 셀룰러 기술[예: 글로벌 이동 통신 시스템(GSM), 코드 분할 다중 액세스(CDMA) • 일반 패킷 라디오 서비스(GPRS)] • 위성 통신	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.1	다음과 같은 개방형 공용 네트워크를 통해 전송하는 동안 강력한 암호화 및 보안 프로토콜을 사용하여 민감한 카드 소지자 데이터를 보호합니다. • 신뢰할 수 있는 키와 인증서만 허용됩니다. • 사용 중인 프로토콜은 보안 버전 또는 구성만 지원합니다. • 암호화 강도는 사용 중인 암호화 방법에 적합합니다. 개방형 공용 네트워크의 예로는 다음이 포함되며 이에 국한되지 않습니다. • 인터넷 • 802.11 및 Bluetooth를 포함한 무선 기술 • 셀룰러 기술[예: 글로벌 이동 통신 시스템(GSM), 코드 분할 다중 액세스(CDMA) • 일반 패킷 라디오 서비스(GPRS)] • 위성 통신	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.2	공급업체에서 제공하는 해당 보안 패치를 설치하여 모든 시스템 구성 요소 및 소프트웨어가 알려진 취약성으로부터 보호되는지 확인합니다. 출시 후 1개월 이내에 주요 보안 패치를 설치합니다. 참고: 요구 사항 6.1에 정의된 위험 순위 프로세스에 따라 중요 보안 패치를 식별해야 합니다.	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
6.2	공급업체에서 제공하는 해당 보안 패치를 설치하여 모든 시스템 구성 요소 및 소프트웨어가 알려진 취약성으로부터 보호되는지 확인합니다. 출시 후 1개월 이내에 주요 보안 패치를 설치합니다. 참고: 요구 사항 6.1에 정의된 위험 순위 프로세스에 따라 중요 보안 패치를 식별해야 합니다.	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.2	공급업체에서 제공하는 해당 보안 패치를 설치하여 모든 시스템 구성 요소 및 소프트웨어가 알려진 취약성으로부터 보호되는지 확인합니다. 출시 후 1개월 이내에 주요 보안 패치를 설치합니다. 참고: 요구 사항 6.1에 정의된 위험 순위 프로세스에 따라 중요 보안 패치를 식별해야 합니다.	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.
6.2	공급업체에서 제공하는 해당 보안 패치를 설치하여 모든 시스템 구성 요소 및 소프트웨어가 알려진 취약성으로부터 보호되는지 확인합니다. 출시 후 1개월 이내에 주요 보안 패치를 설치합니다. 참고: 요구 사항 6.1에 정의된 위험 순위 프로세스에 따라 중요 보안 패치를 식별해야 합니다.	ecs-fargate-latest-platform-version	보안 업데이트 및 패치는 AWS Fargate 작업에 자동으로 배포됩니다. AWS Fargate 플랫폼 버전에 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS 패치합니다. AWS Fargate를 실행하는 Amazon Elastic Container Service(ECS) 태스크의 패치 관리를 지원하려면 최신 플랫폼 버전을 사용하도록 서비스 독립 실행형 태스크를 업데이트합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.2	공급업체에서 제공하는 해당 보안 패치를 설치하여 모든 시스템 구성 요소 및 소프트웨어가 알려진 취약성으로부터 보호되는지 확인합니다. 출시 후 1개월 이내에 주요 보안 패치를 설치합니다. 참고: 요구 사항 6.1에 정의된 위험 순위 프로세스에 따라 중요 보안 패치를 식별해야 합니다.	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.2	공급업체에서 제공하는 해당 보안 패치를 설치하여 모든 시스템 구성 요소 및 소프트웨어가 알려진 취약성으로부터 보호되는지 확인합니다. 출시 후 1개월 이내에 주요 보안 패치를 설치합니다. 참고: 요구 사항 6.1에 정의된 위험 순위 프로세스에 따라 중요 보안 패치를 식별해야 합니다.	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.3.2	프로덕션 또는 고객에게 릴리스하기 전에 사용자 지정 코드를 검토하여 수동 또는 자동 프로세스를 사용하여 잠재적인 코딩 취약성을 식별합니다. • 코드 변경 사항은 최초 코드 작성자가 아닌 개인 및 코드 검토 기법 및 보안 코딩 관행에 대해 잘 아는 개인이 검토합니다. • 코드 검토는 보안 코딩 지침에 따라 코드가 개발되었는지 확인합니다. • 릴리스 전에 적절한 수정 사항이 구현됩니다. • 코드 검토 결과는 출시 전에 경영진이 검토 및 승인합니다. (다음 페이지에 계속)	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository(ECR) 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.6	공개 웹 애플리케이션의 경우 다음 방법 중 하나를 사용하여 새로운 위협과 취약성을 지속적으로 해결하고 알려진 공격으로부터 애플리케이션을 보호하세요. • 수동 또는 자동화된 애플리케이션 취약성 보안 평가 도구 또는 방법으로 공개 웹 애플리케이션을 적어도 매년 그리고 변경 후에 검토합니다. 참고: 이 평가는 요구 사항 11.2에 대해 수행된 취약성 검사와 동일하지 않습니다. • 공개 웹 애플리케이션 앞에 웹 기반 공격(예: 웹 애플리케이션 방화벽)을 탐지하고 방지하는 자동화된 기술 솔루션을 설치하여 모든 트래픽을 지속적으로 확인합니다.	alb-desync-mode-check	HTTP 비동기 취약성으로부터 애플리케이션을 보호하려면 애플리케이션 로드 밸런서에서 HTTP 비동기화 완화 모드를 활성화해야 합니다. HTTP 비동기화 문제로 인해 요청 밀수가 발생하고 애플리케이션이 요청 대기열 또는 캐시 중독에 취약해질 수 있습니다. 비동기화 완화 모드에는 모니터링, 방어 및 가장 엄격 모드가 있습니다. 기본 모드는 방어 모드입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.6	공개 웹 애플리케이션의 경우 다음 방법 중 하나를 사용하여 새로운 위협과 취약성을 지속적으로 해결하고 알려진 공격으로부터 애플리케이션을 보호하세요. • 수동 또는 자동화된 애플리케이션 취약성 보안 평가 도구 또는 방법으로 공개 웹 애플리케이션을 적어도 매년 그리고 변경 후에 검토합니다. 참고: 이 평가는 요구 사항 11.2에 대해 수행된 취약성 검사와 동일하지 않습니다. • 공개 웹 애플리케이션 앞에 웹 기반 공격(예: 웹 애플리케이션 방화벽)을 탐지하고 방지하는 자동화된 기술 솔루션을 설치하여 모든 트래픽을 지속적으로 확인합니다.	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.6	공개 웹 애플리케이션의 경우 다음 방법 중 하나를 사용하여 새로운 위협과 취약성을 지속적으로 해결하고 알려진 공격으로부터 애플리케이션을 보호하세요. • 수동 또는 자동화된 애플리케이션 취약성 보안 평가 도구 또는 방법으로 공개 웹 애플리케이션을 적어도 매년 그리고 변경 후에 검토합니다. 참고: 이 평가는 요구 사항 11.2에 대해 수행된 취약성 검사와 동일하지 않습니다. • 공개 웹 애플리케이션 앞에 웹 기반 공격(예: 웹 애플리케이션 방화벽)을 탐지하고 방지하는 자동화된 기술 솔루션을 설치하여 모든 트래픽을 지속적으로 확인합니다.	[api-gw-associated-with-waf](#)	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.6	공개 웹 애플리케이션의 경우 다음 방법 중 하나를 사용하여 새로운 위협과 취약성을 지속적으로 해결하고 알려진 공격으로부터 애플리케이션을 보호하세요. • 수동 또는 자동화된 애플리케이션 취약성 보안 평가 도구 또는 방법으로 공개 웹 애플리케이션을 적어도 매년 그리고 변경 후에 검토합니다. 참고: 이 평가는 요구 사항 11.2에 대해 수행된 취약성 검사와 동일하지 않습니다. • 공개 웹 애플리케이션 앞에 웹 기반 공격(예: 웹 애플리케이션 방화벽)을 탐지하고 방지하는 자동화된 기술 솔루션을 설치하여 모든 트래픽을 지속적으로 확인합니다.	waf-regional-rule-not-empty	AWS WAF에 비어 있지 않은 규칙이 있는지 확인합니다. 조건이 없는 규칙에서는 의도하지 않은 동작이 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.6	공개 웹 애플리케이션의 경우 다음 방법 중 하나를 사용하여 새로운 위협과 취약성을 지속적으로 해결하고 알려진 공격으로부터 애플리케이션을 보호하세요. • 수동 또는 자동화된 애플리케이션 취약성 보안 평가 도구 또는 방법으로 공개 웹 애플리케이션을 적어도 매년 그리고 변경 후에 검토합니다. 참고: 이 평가는 요구 사항 11.2에 대해 수행된 취약성 검사와 동일하지 않습니다. • 공개 웹 애플리케이션 앞에 웹 기반 공격(예: 웹 애플리케이션 방화벽)을 탐지하고 방지하는 자동화된 기술 솔루션을 설치하여 모든 트래픽을 지속적으로 확인합니다.	waf-regional-rulegroup-not-empty	AWS WAF에 비어 있지 않은 규칙 그룹이 있는지 확인합니다. 규칙 그룹이 비어 있으면 의도하지 않은 동작이 발생할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.6	공개 웹 애플리케이션의 경우 다음 방법 중 하나를 사용하여 새로운 위협과 취약성을 지속적으로 해결하고 알려진 공격으로부터 애플리케이션을 보호하세요. • 수동 또는 자동화된 애플리케이션 취약성 보안 평가 도구 또는 방법으로 공개 웹 애플리케이션을 적어도 매년 그리고 변경 후에 검토합니다. 참고: 이 평가는 요구 사항 11.2에 대해 수행된 취약성 검사와 동일하지 않습니다. • 공개 웹 애플리케이션 앞에 웹 기반 공격(예: 웹 애플리케이션 방화벽)을 탐지하고 방지하는 자동화된 기술 솔루션을 설치하여 모든 트래픽을 지속적으로 확인합니다.	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.1	다음을 포함하여 각 역할에 대한 액세스 요구 사항을 정의합니다. • 각 역할이 직무를 위해 액세스해야 하는 시스템 구성 요소 및 데이터 리소스 • 리소스에 액세스하는 데 필요한 권한 수준(예: 사용자, 관리자 등)	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.2	권한 있는 사용자 ID에 대한 액세스를 직무 수행에 필요한 최소 권한으로 제한합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatt erns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.2	권한 있는 사용자 ID에 대한 액세스를 직무 수행에 필요한 최소 권한으로 제한합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.2	권한 있는 사용자 ID에 대한 액세스를 직무 수행에 필요한 최소 권한으로 제한합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.2	권한 있는 사용자 ID에 대한 액세스를 직무 수행에 필요한 최소 권한으로 제한합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
7.1.2	권한 있는 사용자 ID에 대한 액세스를 직무 수행에 필요한 최소 권한으로 제한합니다.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.2	권한 있는 사용자 ID에 대한 액세스를 직무 수행에 필요한 최소 권한으로 제한합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
7.1.2	권한 있는 사용자 ID에 대한 액세스를 직무 수행에 필요한 최소 권한으로 제한합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.1.2	권한 있는 사용자 ID에 대한 액세스를 직무 수행에 필요한 최소 권한으로 제한합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
7.1.2	권한 있는 사용자 ID에 대한 액세스를 직무 수행에 필요한 최소 권한으로 제한합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Managemen t(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 모든 시스템 구성 요소의 범위가 포함되어야 합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	ecs-containers-nonprivileged	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic Container Service(Amazon ECS) 작업 정의에는 승격 권한이 활성화되어 있지 않아야 합니다. 이 파라미터가 true인 경우 컨테이너는 호스트 컨테이너 인스턴스에 대해 승격된 권한을 부여받습니다(루트 사용자와 비슷함).
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	ecs-containers-readonly-access	Amazon Elastic Container Service(ECS) 컨테이너에 대한 읽기 전용 액세스를 활성화하면 최소 권한 원칙을 준수하는 데 도움이 될 수 있습니다. 명시적인 읽기-쓰기 권한이 없는 한, 이 옵션은 컨테이너 인스턴스의 파일 시스템을 수정할 수 없으므로 공격 벡터를 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소에 사용자에게 필요한 사항을 기준으로 액세스를 제한하고 특별히 허용하지 않는 한 '모두 거부'로 설정된 액세스 제어 시스템을 설정합니다. 이 액세스 제어 시스템에는 직무 분류 및 기능에 따른 개인에게 권한 할당이 포함되어야 합니다.	opensearch-access-control-enabled	Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화되었는지 확인합니다. 세분화된 액세스 제어를 통해 Amazon OpenSearch 서비스 도메인에 대한 액세스 권한을 최소한으로 확보할 수 있는 향상된 권한 부여 메커니즘이 제공됩니다. 이를 통해 도메인에 대한 역할 기반 액세스 제어는 물론 인덱스, 문서 및 필드 수준의 보안, OpenSearch Service 대시보드 멀티테넌시 지원, OpenSearch Service 및 Kibana에 대한 HTTP 기본 인증이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.3	기본 설정은 '모두 거부' 입니다.	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.
8.1.1	모든 사용자에게 고유한 ID를 할당한 다음 시스템 구성 요소 또는 카드 소지자 데이터에 액세스하도록 허용합니다.	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1.4	90일 이내에 비활성 사용자 계정을 제거 또는 비활성화합니다.	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	codebuild-project-environment-privileged-check	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있지 않은지 확인합니다. Docker API와 컨테이너의 기본 하드웨어에 대해 의도하지 않은 액세스를 방지하려면 이 설정을 비활성화해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	ecs-no-environment-secrets	보안 모범 사례로서 민감한 정보를 컨테이너에 환경 변수로 전달합니다. Amazon ECS 태스크 정의의 컨테이너 정의에서 AWS Systems Manager Parameter Store 또는 AWS Secrets Manager에 저장된 값을 참조하여 Amazon Elastic Container Service(ECS) 컨테이너에 데이터를 안전하게 주입할 수 있습니다. 그런 다음, 민감한 정보를 환경 변수 또는 컨테이너의 로그 구성으로 노출할 수 있습니다.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
8.2.1	강력한 암호화를 사용하여 모든 시스템 구성 요소에서 전송 및 저장 중에 모든 인증 자격 증명(예: 암호, 구문)을 읽을 수 없도록 처리합니다.	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.3	비밀번호/패스프레이즈는 다음을 충족해야 합니다. • 최소 길이는 7자 이상이어야 합니다. • 숫자와 영문자를 모두 포함합니다. 또는 비밀번호/패스프레이즈의 복잡성과 강도는 최소한 위에 지정된 파라미터와 동등해야 합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 IAM 암호 정책에 대해 RequireUppercaseCharacters(PCI DSS 기본값: false), RequireLowercaseCharacters(PCI DSS 기본값: true), RequireSymbols(PCI DSS 기본값: false), RequireNumbers(PCI DSS 기본값: true), MinimumPasswordLength(PCI DSS 기본값: 7), PasswordReusePrevention(PCI DSS 기본값: 4) 및 MaxPasswordAge(PCI DSS 기본값: 90)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.4	최소 90일에 한 번씩 사용자 암호 및 패스프레이즈를 변경합니다.	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.4	최소 90일에 한 번씩 사용자 암호 및 패스프레이즈를 변경합니다.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 IAM 암호 정책에 대해 RequireUppercaseCharacters(PCI DSS 기본값: false), RequireLowercaseCharacters(PCI DSS 기본값: true), RequireSymbols(PCI DSS 기본값: false), RequireNumbers(PCI DSS 기본값: true), MinimumPasswordLength(PCI DSS 기본값: 7), PasswordReusePrevention(PCI DSS 기본값: 4) 및 MaxPasswordAge(PCI DSS 기본값: 90)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.4	최소 90일에 한 번씩 사용자 암호 및 패스프레이즈를 변경합니다.	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.5	최근 사용한 네 개의 비밀번호/패스프레이즈와 동일한 새 비밀번호/패스프레이즈를 제출하지 못하게 하세요.	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 IAM 암호 정책에 대해 RequireUppercaseCharacters(PCI DSS 기본값: false), RequireLowercaseCharacters(PCI DSS 기본값: true), RequireSymbols(PCI DSS 기본값: false), RequireNumbers(PCI DSS 기본값: true), MinimumPasswordLength(PCI DSS 기본값: 7), PasswordReusePrevention(PCI DSS 기본값: 4) 및 MaxPasswordAge(PCI DSS 기본값: 90)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.1	관리 권한이 있는 담당자를 위해 콘솔이 아닌 모든 액세스에 대한 다중 인증을 CDE에 통합합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
8.3.1	관리 권한이 있는 담당자를 위해 콘솔이 아닌 모든 액세스에 대한 다중 인증을 CDE에 통합합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.1	관리 권한이 있는 담당자를 위해 콘솔이 아닌 모든 액세스에 대한 다중 인증을 CDE에 통합합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
8.3.1	관리 권한이 있는 담당자를 위해 콘솔이 아닌 모든 액세스에 대한 다중 인증을 CDE에 통합합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	엔티티 네트워크 외부에서 발생하는 모든 원격 네트워크 액세스(사용자 및 관리자, 지원 또는 유지 관리를 위한 타사 액세스 포함)에 대해 다중 인증을 통합합니다.	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.
8.3.2	엔티티 네트워크 외부에서 발생하는 모든 원격 네트워크 액세스(사용자 및 관리자, 지원 또는 유지 관리를 위한 타사 액세스 포함)에 대해 다중 인증을 통합합니다.	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	엔티티 네트워크 외부에서 발생하는 모든 원격 네트워크 액세스(사용자 및 관리자, 지원 또는 유지 관리를 위한 타사 액세스 포함)에 대해 다중 인증을 통합합니다.	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
8.3.2	엔티티 네트워크 외부에서 발생하는 모든 원격 네트워크 액세스(사용자 및 관리자, 지원 또는 유지 관리를 위한 타사 액세스 포함)에 대해 다중 인증을 통합합니다.	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA를 통해 사용자 이름 및 암호에 보호 계층이 한 단계 더 추가됩니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.1	감사 추적을 구현하여 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자에게 연결합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
10.2.1	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '카드 소지자 데이터에 대한 모든 개별 사용자 액세스' 이벤트를 다시 구성합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '카드 소지자 데이터에 대한 모든 개별 사용자 액세스' 이벤트를 다시 구성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '카드 소지자 데이터에 대한 모든 개별 사용자 액세스' 이벤트를 다시 구성합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '카드 소지자 데이터에 대한 모든 개별 사용자 액세스' 이벤트를 다시 구성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
10.2.1	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '카드 소지자 데이터에 대한 모든 개별 사용자 액세스' 이벤트를 다시 구성합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '카드 소지자 데이터에 대한 모든 개별 사용자 액세스' 이벤트를 다시 구성합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
10.2.1	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '카드 소지자 데이터에 대한 모든 개별 사용자 액세스' 이벤트를 다시 구성합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '카드 소지자 데이터에 대한 모든 개별 사용자 액세스' 이벤트를 다시 구성합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
10.2.1	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '카드 소지자 데이터에 대한 모든 개별 사용자 액세스' 이벤트를 다시 구성합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '카드 소지자 데이터에 대한 모든 개별 사용자 액세스' 이벤트를 다시 구성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '카드 소지자 데이터에 대한 모든 개별 사용자 액세스' 이벤트를 다시 구성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '루트 또는 관리 권한이 있는 개인이 수행하는 모든 작업' 이벤트를 다시 구성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '루트 또는 관리 권한이 있는 개인이 수행하는 모든 작업' 이벤트를 다시 구성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
10.2.2	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '루트 또는 관리 권한이 있는 개인이 수행하는 모든 작업' 이벤트를 다시 구성합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '루트 또는 관리 권한이 있는 개인이 수행하는 모든 작업' 이벤트를 다시 구성합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
10.2.2	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '루트 또는 관리 권한이 있는 개인이 수행하는 모든 작업' 이벤트를 다시 구성합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '루트 또는 관리 권한이 있는 개인이 수행하는 모든 작업' 이벤트를 다시 구성합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
10.2.2	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '루트 또는 관리 권한이 있는 개인이 수행하는 모든 작업' 이벤트를 다시 구성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '루트 또는 관리 권한이 있는 개인이 수행하는 모든 작업' 이벤트를 다시 구성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.3	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '모든 감사 추적에 대한 액세스' 이벤트를 다시 구성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.3	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '모든 감사 추적에 대한 액세스' 이벤트를 다시 구성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
10.2.3	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '모든 감사 추적에 대한 액세스' 이벤트를 다시 구성합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.3	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '모든 감사 추적에 대한 액세스' 이벤트를 다시 구성합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
10.2.3	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '모든 감사 추적에 대한 액세스' 이벤트를 다시 구성합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.3	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '모든 감사 추적에 대한 액세스' 이벤트를 다시 구성합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
10.2.3	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '모든 감사 추적에 대한 액세스' 이벤트를 다시 구성합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.3	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '모든 감사 추적에 대한 액세스' 이벤트를 다시 구성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.3	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '모든 감사 추적에 대한 액세스' 이벤트를 다시 구성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.3	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '모든 감사 추적에 대한 액세스' 이벤트를 다시 구성합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
10.2.4	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '잘못된 논리적 액세스 시도' 이벤트를 다시 구성합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.4	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '잘못된 논리적 액세스 시도' 이벤트를 다시 구성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.4	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '잘못된 논리적 액세스 시도' 이벤트를 다시 구성합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.4	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '잘못된 논리적 액세스 시도' 이벤트를 다시 구성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
10.2.4	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '잘못된 논리적 액세스 시도' 이벤트를 다시 구성합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.4	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '잘못된 논리적 액세스 시도' 이벤트를 다시 구성합니다..	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
10.2.4	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '잘못된 논리적 액세스 시도' 이벤트를 다시 구성합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.4	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '잘못된 논리적 액세스 시도' 이벤트를 다시 구성합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
10.2.4	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '잘못된 논리적 액세스 시도' 이벤트를 다시 구성합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.4	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '잘못된 논리적 액세스 시도' 이벤트를 다시 구성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.4	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '잘못된 논리적 액세스 시도' 이벤트를 다시 구성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.5	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '식별 및 인증 메커니즘의 사용 및 변경(새 계정 생성 및 권한 상승 포함), 루트 또는 관리 권한이 있는 계정 변경, 추가 또는 삭제' 이벤트를 다시 구성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.5	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '식별 및 인증 메커니즘의 사용 및 변경(새 계정 생성 및 권한 상승 포함), 루트 또는 관리 권한이 있는 계정 변경, 추가 또는 삭제' 이벤트를 다시 구성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
10.2.5	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '식별 및 인증 메커니즘의 사용 및 변경(새 계정 생성 및 권한 상승 포함), 루트 또는 관리 권한이 있는 계정 변경, 추가 또는 삭제' 이벤트를 다시 구성합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.5	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '식별 및 인증 메커니즘의 사용 및 변경(새 계정 생성 및 권한 상승 포함), 루트 또는 관리 권한이 있는 계정 변경, 추가 또는 삭제' 이벤트를 다시 구성합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
10.2.5	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '식별 및 인증 메커니즘의 사용 및 변경(새 계정 생성 및 권한 상승 포함), 루트 또는 관리 권한이 있는 계정 변경, 추가 또는 삭제' 이벤트를 다시 구성합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.5	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '식별 및 인증 메커니즘의 사용 및 변경(새 계정 생성 및 권한 상승 포함), 루트 또는 관리 권한이 있는 계정 변경, 추가 또는 삭제' 이벤트를 다시 구성합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
10.2.5	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '식별 및 인증 메커니즘의 사용 및 변경(새 계정 생성 및 권한 상승 포함), 루트 또는 관리 권한이 있는 계정 변경, 추가 또는 삭제' 이벤트를 다시 구성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.5	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '식별 및 인증 메커니즘의 사용 및 변경(새 계정 생성 및 권한 상승 포함), 루트 또는 관리 권한이 있는 계정 변경, 추가 또는 삭제' 이벤트를 다시 구성합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.6	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '감사 로그의 초기화, 중지 또는 일시 중지' 이벤트를 다시 구성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.6	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '감사 로그의 초기화, 중지 또는 일시 중지' 이벤트를 다시 구성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
10.2.6	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '감사 로그의 초기화, 중지 또는 일시 중지' 이벤트를 다시 구성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.7	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '시스템 수준 객체 생성 및 삭제' 이벤트를 다시 구성합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
10.2.7	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '시스템 수준 객체 생성 및 삭제' 이벤트를 다시 구성합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.7	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '시스템 수준 객체 생성 및 삭제' 이벤트를 다시 구성합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
10.2.7	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '시스템 수준 객체 생성 및 삭제' 이벤트를 다시 구성합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.7	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '시스템 수준 객체 생성 및 삭제' 이벤트를 다시 구성합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
10.2.7	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '시스템 수준 객체 생성 및 삭제' 이벤트를 다시 구성합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.7	모든 시스템 구성 요소에 대해 자동 감사 추적을 구현하여 '시스템 수준 객체 생성 및 삭제' 이벤트를 다시 구성합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하기 위해 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업을 기록합니다.
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	이벤트마다 모든 시스템 구성 요소에 대해 적어도 '사용자 식별' 감사 추적 항목을 기록합니다.	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
10.5	감사 추적을 안전하게 보호하여 변경할 수 없도록 하세요.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.5	감사 추적을 안전하게 보호하여 변경할 수 없도록 하세요.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
10.5	감사 추적을 안전하게 보호하여 변경할 수 없도록 하세요.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.5.2	감사 추적 파일을 무단 수정으로부터 보호합니다.	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.5.2	감사 추적 파일을 무단 수정으로부터 보호합니다.	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
10.5.2	감사 추적 파일을 무단 수정으로부터 보호합니다.	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
10.5.3	감사 추적 파일을 중앙 집중식 로그 서버 또는 변경하기 어려운 미디어에 지체 없이 백업합니다.	s3-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다 (예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS 구성 규칙	지침
10.5.3	감사 추적 파일을 중앙 집중식 로그 서버 또는 변경하기 어려운 미디어에 지체 없이 백업합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.5.3	감사 추적 파일을 중앙 집중식 로그 서버 또는 변경하기 어려운 미디어에 지체 없이 백업합니다.	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
10.5.3	감사 추적 파일을 중앙 집중식 로그 서버 또는 변경하기 어려운 미디어에 지체 없이 백업합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.5.5	로그에 대해 파일 무결성 모니터링이나 변경 감지 소프트웨어를 사용하여 기존 로그 데이터가 변경되는 경우 알림을 생성하도록 합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.5.5	로그에 대해 파일 무결성 모니터링이나 변경 감지 소프트웨어를 사용하여 기존 로그 데이터가 변경되는 경우 알림을 생성하도록 합니다.	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
10.7	감사 추적 기록을 최소 1년 동안 보관하고, 이 기록은 최소 3개월 동안 즉시 분석에 사용할 수 있어야 합니다(예: 온라인, 아카이브 또는 백업에서 복원 가능).	s3-lifecycle-policy-check	Amazon S3 수명 주기 정책이 객체 수명 주기 동안 Amazon S3에서 수행하려는 작업을 정의하도록 구성됩니다(예: 객체를 다른 스토리지 클래스로 이전, 객체 보관, 지정된 기간이 경과한 후 객체 삭제).

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7	감사 추적 기록을 최소 1년 동안 보관하고, 이 기록은 최소 3개월 동안 즉시 분석에 사용할 수 있어야 합니다(예: 온라인, 아카이브 또는 백업에서 복원 가능).	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.2.3	내부 및 외부 스캔을 수행하고 중요한 변경 후 필요에 따라 다시 스캔합니다. 스캔은 자격을 갖춘 직원이 수행해야 합니다.	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository(ECR) 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 활성화하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.
11.4	침입 탐지 및/또는 침입 방지 기술을 사용하여 네트워크 침입을 탐지 및/또는 방지합니다. 카드 소지자 데이터 환경의 경계와 카드 소지자 데이터 환경의 중요 지점에서 모든 트래픽을 모니터링하고 보안 침해가 의심되는 경우 직원에게 알립니다. 모든 침입 탐지 및 방지 엔진, 기준, 서명을 최신 상태로 유지합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.4	침입 탐지 및/또는 침입 방지 기술을 사용하여 네트워크 침입을 탐지 및/또는 방지합니다. 카드 소지자 데이터 환경의 경계와 카드 소지자 데이터 환경의 중요 지점에서 모든 트래픽을 모니터링하고 보안 침해가 의심되는 경우 직원에게 알립니다. 모든 침입 탐지 및 방지 엔진, 기준, 서명을 최신 상태로 유지합니다.	netfw-policy-rule-group-associated	AWS Network Firewall 정책은 방화벽이 Amazon VPC에서 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하여 패킷과 트래픽 흐름을 필터링하고 기본 트래픽 처리를 정의합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.5	변경 감지 메커니즘(예: 파일 무결성 모니터링 도구)을 배포하여 중요한 시스템 파일, 구성 파일 또는 콘텐츠 파일의 무단 수정(변경, 추가, 삭제 포함)을 담당자에게 알리고, 중요 파일 비교를 매주 이상 수행하도록 소프트웨어를 구성합니다.	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.5	변경 감지 메커니즘(예: 파일 무결성 모니터링 도구)을 배포하여 중요한 시스템 파일, 구성 파일 또는 콘텐츠 파일의 무단 수정(변경, 추가, 삭제 포함)을 담당자에게 알리고, 중요 파일 비교를 매주 이상 수행하도록 소프트웨어를 구성합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

템플릿

템플릿은 GitHub: PCI DSS 3.2.1 운영 모범 사례에서 확인할 수 있습니다.

PCI DSS 4.0 운영 모범 사례(글로벌 리소스 유형 제외)

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Payment Card Industry Data Security Standard(PCI DSS) 4.0(글로벌 리소스 유형 제외)과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 AWS Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 PCI DSS 제어와 관련이 있습니다. PCI DSS 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.5	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	AWS Transfer Family로 생성된 서버가 엔드포인트 연결에 FTP를 사용하지 않는지 확인합니다. 엔드포인트 연결을 위한 서버 프로토콜이 FTP를 활성화한 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장

제어 ID	제어 설명	AWS 구성 규칙	지침
			기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙이 웹 ACL과 연결되지 않은 경우 규칙은 AWS AppSync API에 대한 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift 클러스터에 'enhanced VpcRouting'이 활성화되어 있는지 확인합니다. 'enhanced VpcRouting'이 활성화되지 않았거나, configuration.enhancedVpcRouting 필드가 'false'인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙이 웹 ACL과 연결되지 않은 경우 규칙은 AWS AppSync API에 대한 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift 클러스터에 'enhanced VpcRouting'이 활성화되어 있는지 확인합니다. 'enhanced VpcRouting'이 활성화되지 않았거나, configuration.enhancedVpcRouting 필드가 'false'인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙이 웹 ACL과 연결되지 않은 경우 규칙은 AWS AppSync API에 대한 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
1.4.1	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.1	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift 클러스터에 'enhancedVpcRouting'이 활성화되어 있는지 확인합니다. 'enhancedVpcRouting'이 활성화되지 않았거나, configuration.enhancedVpcRouting 필드가 'false'인 경우 규칙은 NON_COMPLIANT입니다.
1.4.1	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift 클러스터에 'enhancedVpcRouting'이 활성화되어 있는지 확인합니다. 'enhancedVpcRouting'이 활성화되지 않았거나, configuration.enhancedVpcRouting 필드가 'false'인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙이 웹 ACL과 연결되지 않은 경우 규칙은 AWS AppSync API에 대한 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
1.4.3	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.3	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.
1.4.3	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-full-packets	AWS Network Firewall 정책이 전체 패킷에 대해 사용자 정의 기본 상태 비저장 작업으로 구성되어 있는지 확인합니다. 전체 기본 상태 비저장 작업이 사용자 정의 기본 상태 비저장 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.4	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.
1.4.4	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift 클러스터에 'enhancedVpcRouting'이 활성화되어 있는지 확인합니다. 'enhancedVpcRouting'이 활성화되지 않았거나, configuration.enhancedVpcRouting 필드가 'false'인 경우 규칙은 NON_COMPLIANT입니다.
1.4.4	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.5	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	ecs-task-definition-pid-mode-check	ECSTaskDefinitions가 호스트의 프로세스 네임스페이스를 Amazon Elastic Container Service(Amazon ECS) 컨테이너와 공유하도록 구성되어 있는지 확인합니다. pidMode 파라미터가 'host'로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.4.5	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	ec2-launch-template-public-ip-disabled	Amazon EC2 시작 템플릿이 네트워크 인터페이스에 퍼블릭 IP 주소를 할당하도록 설정되지 않았는지 확인합니다. EC2 시작 템플릿의 기본 버전에 'AssociatePublicIpAddress'가 'true'로 설정된 네트워크 인터페이스가 하나 이상 있는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙이 웹 ACL과 연결되지 않은 경우 규칙은 AWS AppSync API에 대한 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT 입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT 입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT 입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT입니다.
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 수동 DB 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. 기존 및 신규 Neptune 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	aurora-resources-protected-by-backup-plan	Amazon Aurora DB 클러스터가 백업 계획으로 보호되고 있는지 확인합니다. Amazon Relational Database Service(RDS) 데이터베이스 클러스터가 백업 계획에 의해 보호되고 있지 않을 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	db-instance-backup-enabled	RDS DB 인스턴스에 백업이 활성화되어 있는지 확인합니다. 이 규칙은 필요에 따라 백업 보존 기간과 백업 기간을 확인합니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	dynamodb-in-backup-plan	Amazon DynamoDB 테이블이 AWS 백업 계획에 있는지 확인합니다. Amazon DynamoDB 테이블이 AWS 백업 계획에 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	dynamodb-resources-protected-by-backup-plan	Amazon DynamoDB 테이블이 백업 계획으로 보호되는지 확인합니다. DynamoDB 테이블을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT 입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	ebs-in-backup-plan	AWS 백업의 백업 계획에 Amazon Elastic Block Store(Amazon EBS) 볼륨이 추가되었는지 확인합니다. Amazon EBS 볼륨이 백업 계획에 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	ebs-resources-protected-by-backup-plan	Amazon Elastic Block Store(Amazon EBS) 볼륨이 백업 계획으로 보호되는지 확인합니다. Amazon EBS 볼륨을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	ec2-resources-protected-by-backup-plan	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스가 백업 계획으로 보호되는지 확인합니다. Amazon EC2 인스턴스를 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT 입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	efs-resources-protected-by-backup-plan	Amazon Elastic File System(Amazon EFS) 파일 시스템이 백업 계획으로 보호되는지 확인합니다. EFS 파일 시스템을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	elasticache-redis-cluster-automatic-backup-check	Amazon ElastiCache Redis 클러스터에 자동 백업이 설정되어 있는지 확인합니다. Redis 클러스터에 대한 SnapshotRetentionLimit가 SnapshotRetentionPeriod 파라미터보다 작으면 규칙은 NON_COMPLIANT입니다. 예를 들어 파라미터가 15인 경우 snapshotRetentionPeriod가 0~15이면 규칙이 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	fsx-resources-protected-by-backup-plan	Amazon FSx 파일 시스템이 백업 계획에 의해 보호되고 있는지 확인합니다. Amazon FSx 파일 시스템을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-backup-retention-check	Amazon Neptune DB 클러스터 보존 기간이 특정 일수로 설정되어 있는지 확인합니다. 보존 기간이 파라미터에서 지정된 값보다 짧은 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	rds-in-backup-plan	Amazon Relational Database Service(Amazon RDS) 데이터베이스가 AWS 백업 계획에 있는지 확인합니다. Amazon RDS 데이터베이스가 AWS 백업 계획에 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	redshift-backup-enabled	클러스터에 대해 Amazon Redshift 자동 스냅샷이 활성화되어 있는지 확인합니다. automatedSnapshotRetentionPeriod의 값이 MaxRetentionPeriod보다 크거나 MinRetentionPeriod보다 작거나 값이 0인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-resources-protected-by-backup-plan	Amazon Simple Storage Service(Amazon S3) 버킷이 백업 플랜에 의해 보호되는지 확인합니다. Amazon S3 버킷을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	db-instance-backup-enabled	RDS DB 인스턴스에 백업이 활성화되어 있는지 확인합니다. 이 규칙은 필요에 따라 백업 보존 기간과 백업 기간을 확인합니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.4	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-bucket-default-lock-enabled	기본적으로 S3 버킷에 잠금이 활성화되어 있는지 확인합니다. 잠금이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.4	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-bucket-versioning-enabled	S3 버킷에 버전 관리가 활성화되어 있는지 확인합니다. 이 규칙은 필요에 따라 S3 버킷에 MFA 삭제가 활성화되어 있는지 확인합니다.
10.3.4	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT입니다.
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig. CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig. CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig. CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.3	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.5.1	감사 로그 기록은 유지되며 분석에 사용할 수 있습니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT입니다.
10.5.1	감사 로그 기록은 유지되며 분석에 사용할 수 있습니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.5.1	감사 로그 기록은 유지되며 분석에 사용할 수 있습니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.5.1	감사 로그 기록은 유지되며 분석에 사용할 수 있습니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.5.1	감사 로그 기록은 유지되며 분석에 사용할 수 있습니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT 입니다.
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig. CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.5.2	네트워크 침입 및 예기치 않은 파일 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
11.5.2	네트워크 침입 및 예기치 않은 파일 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
11.5.2	네트워크 침입 및 예기치 않은 파일 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	지정된 지표 이름의 CloudWatch 경보 설정이 지정한 설정과 일치하는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.5.2	네트워크 침입 및 예기치 않은 파일 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
11.6.1	결제 페이지의 무단 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.6.1	결제 페이지의 무단 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
11.6.1	결제 페이지의 무단 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	지정된 지표 이름의 CloudWatch 경보 설정이 지정한 설정과 일치하는지 확인합니다.
11.6.1	결제 페이지의 무단 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.10.5	CDE에 영향을 미칠 수 있는 의심되고 확인된 보안 사고에 즉시 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
12.10.5	CDE에 영향을 미칠 수 있는 의심되고 확인된 보안 사고에 즉시 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
12.10.5	CDE에 영향을 미칠 수 있는 의심되고 확인된 보안 사고에 즉시 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	지정된 지표 이름의 CloudWatch 경보 설정이 지정한 설정과 일치하는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.10.5	CDE에 영향을 미칠 수 있는 의심되고 확인된 보안 사고에 즉시 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
12.4.2.1	PCI DSS 규정 준수를 관리합니다. (PCI-DSS-v4.0)	service-catalog-shared-within-organization	AWS Organizations와의 통합이 활성화된 경우 AWS Service Catalog가 조직(단일 단위로 취급되는 AWS 계정 모음)과 포트폴리오를 공유하는지 확인합니다. 공유의 `Type` 값이 `ACCOUNT`인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.5	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	AWS Transfer Family로 생성된 서버가 엔드포인트 연결에 FTP를 사용하지 않는지 확인합니다. 엔드포인트 연결을 위한 서버 프로토콜이 FTP를 활성화한 경우 규칙은 NON_COMPLIANT입니다.
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis 데이터 스토어용 AWS Database Migration Service(AWS DMS) 엔드포인트가 다른 엔드포인트와 통신하는 데이터의 TLS/SSL 암호화에 대해 활성화되어 있는지 확인합니다. TLS/SSL 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK 클러스터가 클러스터의 브로커 노드와 함께 HTTPS(TLS)를 사용하여 전송 중 암호화를 적용하는지 확인합니다. 클러스터 내 브로커 노드 연결에 대해 일반 텍스트 통신이 활성화된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service(AWS DMS) 엔드포인트가 SSL 연결로 구성되어 있는지 확인합니다. AWS DMS에 SSL 연결이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.2.1	계정 데이터의 저장은 최소한으로 유지됩니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.
3.2.1	계정 데이터의 저장은 최소한으로 유지됩니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1	계정 데이터의 저장은 최소한으로 유지됩니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.2.1	계정 데이터의 저장은 최소한으로 유지됩니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.
3.3.1.1	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1.1	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.
3.3.1.1	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.3.1.1	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.
3.3.1.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.
3.3.1.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.
3.3.2	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.
3.3.2	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.2	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.3.2	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.
3.3.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.
3.3.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.3.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-rest	Amazon Athena 작업 그룹이 저장 시 암호화되는지 확인합니다. Athena 작업 그룹에 대해 저장 데이터 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Amazon Neptune DB 클러스터에 암호화된 스냅샷이 있는지 확인합니다. Neptune 클러스터에 암호화된 스냅샷이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Amazon Redshift 클러스터가 암호화에 지정된 AWS Key Management Service(AWS KMS) 키를 사용하고 있는지 확인합니다. 암호화가 활성화되어 있고 kmsKeyArn 파라미터에 제공된 키로 클러스터가 암호화된 경우 규칙은 COMPLIANT입니다. 클러스터가 암호화되지 않거나 다른 키로 암호화된 경우 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	codebuild-project-s3-logs-encrypted	Amazon S3 Logs로 구성된 AWS CodeBuild 프로젝트에 해당 로그에 대한 암호화가 활성화되어 있는지 확인합니다. CodeBuild 프로젝트의 S3LogsConfig에서 'encryptionDisabled'가 'true'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	eks-secrets-encrypted	Amazon Elastic Kubernetes Service 클러스터가 AWS Key Management Service(KMS) 키를 사용하여 Kubernetes 보안 암호를 암호화하도록 구성되어 있는지 확인합니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	api-gw-cache-enabled-and-encrypted	Amazon API Gateway 단계의 모든 메서드에 캐시가 활성화되어 있고 캐시가 암호화되어 있는지 확인합니다. Amazon API Gateway 단계에 캐싱이 구성되지 않았거나, 캐시가 암호화되지 않은 메서드가 있을 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블이 AWS Key Management Service(KMS)로 암호화되어 있는지 확인합니다. Amazon DynamoDB 테이블이 AWS KMS로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다. 암호화된 AWS KMS 키가 kmsKeyArns 입력 파라미터에 없는 경우에도 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	프로젝트에 환경 변수 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 포함되어 있지 않은지 확인합니다. 프로젝트 환경 변수에 일반 텍스트 자격 증명이 포함된 경우, 이 규칙은 NON_COMPLIANT로 간주됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Amazon EKS 클러스터가 KMS를 사용하여 암호화된 AWS Kubernetes 보안 암호를 갖도록 구성되지 않았는지 확인합니다. EKS 클러스터에 encryptionConfig 리소스가 없거나 encryptionConfig이 리소스를 보안 키로 명명하지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Amazon Kinesis 스트림이 서버 측 암호화를 사용하여 저장 시 암호화되는지 확인합니다. 'StreamEncryption'이 없는 경우 Kinesis 스트림의 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-encrypted	Amazon Neptune DB 클러스터에 스토리지 암호화가 활성화되어 있는지 확인합니다. 스토리지 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.5.1.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 수동 DB 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. 기존 및 신규 Neptune 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.6.1	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1.2	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.6.1.2	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1.3	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.6.1.3	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1.4	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.6.1.4	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.1	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-certificate-rsa-check	AWS Certificate Manager(ACM)에서 관리하는 RSA 인증서의 키 길이가 '2048'비트 이상인지 확인합니다. 최소 키 길이가 2048비트 미만인 경우 규칙은 NON_COMPLIANT입니다.
3.7.1	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.1	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
3.7.2	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.2	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
3.7.4	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.4	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
3.7.6	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.6	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
3.7.7	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.7	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis 데이터 스토어용 AWS Database Migration Service(AWS DMS) 엔드포인트가 다른 엔드포인트와 통신하는 데이터의 TLS/SSL 암호화에 대해 활성화되어 있는지 확인합니다. TLS/SSL 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK 클러스터가 클러스터의 브로커 노드와 함께 HTTPS(TLS)를 사용하여 전송 중 암호화를 적용하는지 확인합니다. 클러스터 내 브로커 노드 연결에 대해 일반 텍스트 통신이 활성화된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service(AWS DMS) 엔드포인트가 SSL 연결로 구성되어 있는지 확인합니다. AWS DMS에 SSL 연결이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis 데이터 스토어용 AWS Database Migration Service(AWS DMS) 엔드포인트가 다른 엔드포인트와 통신하는 데이터의 TLS/SSL 암호화에 대해 활성화되어 있는지 확인합니다. TLS/SSL 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK 클러스터가 클러스터의 브로커 노드와 함께 HTTPS(TLS)를 사용하여 전송 중 암호화를 적용하는지 확인합니다. 클러스터 내 브로커 노드 연결에 대해 일반 텍스트 통신이 활성화된 경우 규칙은 NON_COMPLIANT입니다.
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service(AWS DMS) 엔드포인트가 SSL 연결로 구성되어 있는지 확인합니다. AWS DMS에 SSL 연결이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.3.3	보안 취약성을 식별하고 해결합니다. (PCI-DSS-v4.0)	lambda-function-settings-check	런타임, 역할, 제한 시간 및 메모리 크기에 대한 AWS Lambda 함수 설정이 예상 값과 일치하는지 확인합니다. 규칙은 '이미지' 패키지 유형이 있는 함수와 런타임이 'OS 전용 런타임'으로 설정된 함수를 무시합니다. Lambda 함수 설정이 예상 값과 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.
6.3.3	보안 취약성을 식별하고 해결합니다. (PCI-DSS-v4.0)	eks-cluster-oldest-supported-version	Amazon Elastic Kubernetes Service(EKS) 클러스터가 지원되는 가장 오래된 버전을 실행하고 있지 않는지 확인합니다. EKS 클러스터가 지원되는 가장 오래된 버전(파라미터 'oldestVersionSupported'와 같음)을 실행하는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4.1	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙은 웹 ACL과 연결되지 않은 경우 AWS AppSync API에 대한 NON_COMPLIANT입니다.
6.4.1	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	wafv2-webacl-not-empty	WAFv2 리전 웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
6.4.1	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	wafv2-rulegroup-not-empty	WAFv2 규칙 그룹에 규칙이 포함되어 있는지 확인합니다. WAFv2 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4.2	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙은 웹 ACL과 연결되지 않은 경우 AWS AppSync API에 대한 NON_COMPLIANT입니다.
6.4.2	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	wafv2-webacl-not-empty	WAFv2 리전 웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
6.4.2	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	wafv2-rulegroup-not-empty	WAFv2 규칙 그룹에 규칙이 포함되어 있는지 확인합니다. WAFv2 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.5.5	모든 시스템 구성 요소에 대한 변경 사항을 안전하게 관리합니다. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-disabled	Lambda Compute Platform의 배포 그룹이 기본 배포 구성을 사용하지 않는지 확인합니다. 배포 그룹이 배포 구성 'CodeDeployDefault.LambdaAllAtOnce'를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
6.5.6	모든 시스템 구성 요소에 대한 변경 사항을 안전하게 관리합니다. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-disabled	Lambda Compute Platform의 배포 그룹이 기본 배포 구성을 사용하지 않는지 확인합니다. 배포 그룹이 배포 구성 'CodeDeployDefault.LambdaAllAtOnce'를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
7.2.4	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	secretsmanager-secret-unused	지정된 일수 내에 AWS Secrets Manager 보안 암호에 액세스했는지 확인합니다. 'unusedForDays' 일수 내에 보안 암호에 액세스하지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
7.2.5.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	secretsmanager-secret-unused	지정된 일수 내에 AWS Secrets Manager 보안 암호에 액세스했는지 확인합니다. 'unusedForDays' 일수 내에 보안 암호에 액세스하지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.6	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.2.6	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
8.2.1	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.1	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud(EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되고 있지 않는지 확인합니다. 실행 중인 EC2 인스턴스가 키 페어를 사용하여 시작된 경우 규칙은 NON_COMPLIANT입니다.
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud(EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되고 있지 않는지 확인합니다. 실행 중인 EC2 인스턴스가 키 페어를 사용하여 시작된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	프로젝트에 환경 변수 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 포함되어 있지 않은지 확인합니다. 프로젝트 환경 변수에 일반 텍스트 자격 증명이 포함된 경우, 이 규칙은 NON_COMPLIANT로 간주됩니다.
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-secret-unused	지정된 일수 내에 AWS Secrets Manager 보안 암호에 액세스했는지 확인합니다. 'unusedForDays' 일수 내에 보안 암호에 액세스하지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.2.4	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.4	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud(EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되고 있지 않는지 확인합니다. 실행 중인 EC2 인스턴스가 키 페어를 사용하여 시작된 경우 규칙은 NON_COMPLIANT입니다.
8.2.5	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.2.5	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud(EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되고 있지 않는지 확인합니다. 실행 중인 EC2 인스턴스가 키 페어를 사용하여 시작된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.6	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-secret-unused	지정된 일수 내에 AWS Secrets Manager 보안 암호에 액세스했는지 확인합니다. 'unusedForDays' 일수 내에 보안 암호에 액세스하지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터 버전이 인스턴스 메타데이터 서비스 버전2(IMDSv2)로 구성되었는지 확인합니다. HttpTokens가 선택 사항으로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	autoscaling-launchconfig-requires-imdsv2	IMDSv2만 활성화되어 있는지 확인합니다. 메타데이터 버전이 시작 구성에 포함되어 있지 않거나, 메타데이터 V1과 V2가 둘 다 활성화된 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
8.3.10.1	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	access-keys-rotated	유효한 IAM 액세스 키가 maxAccessKeyAge에 지정된 일수에 따라 교체(변경)되는지 확인합니다. 지정된 기간 내에 액세스 키가 교체되지 않는 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.10.1	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.10.1	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.3.11	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.11	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud(EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되고 있지 않는지 확인합니다. 실행 중인 EC2 인스턴스가 키 페어를 사용하여 시작된 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-rest	Amazon Athena 작업 그룹이 저장 시 암호화되는지 확인합니다. Athena 작업 그룹에 대해 저장 데이터 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Amazon Neptune DB 클러스터에 암호화된 스냅샷이 있는지 확인합니다. Neptune 클러스터에 암호화된 스냅샷이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Amazon Redshift 클러스터가 암호화에 지정된 AWS Key Management Service(AWS KMS) 키를 사용하고 있는지 확인합니다. 암호화가 활성화되어 있고 kmsKeyArn 파라미터에 제공된 키로 클러스터가 암호화된 경우 규칙은 COMPLIANT입니다. 클러스터가 암호화되지 않거나 다른 키로 암호화된 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	codebuild-project-s3-logs-encrypted	Amazon S3 Logs로 구성된 AWS CodeBuild 프로젝트에 해당 로그에 암호화가 활성화되어 있는지 확인합니다. CodeBuild 프로젝트의 S3LogsConfig에서 'encryptionDisabled'가 'true'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis 데이터 스토어용 AWS Database Migration Service(AWS DMS) 엔드포인트가 다른 엔드포인트와 통신하는 데이터의 TLS/SSL 암호화에 활성화되어 있는지 확인합니다. TLS/SSL 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	eks-secrets-encrypted	Amazon Elastic Kubernetes Service 클러스터가 AWS Key Management Service(KMS) 키를 사용하여 Kubernetes 보안 암호를 암호화하도록 구성되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	api-gw-cache-enabled-and-encrypted	Amazon API Gateway 단계의 모든 메서드에 캐시가 활성화되어 있고 캐시가 암호화되어 있는지 확인합니다. Amazon API Gateway 단계에 캐싱이 구성되지 않았거나, 캐시가 암호화되지 않은 메서드가 있을 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블이 AWS Key Management Service(KMS)로 암호화되어 있는지 확인합니다. Amazon DynamoDB 테이블이 AWS KMS로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다. 암호화된 AWS KMS 키가 kmsKeyArns 입력 파라미터에 없는 경우에도 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	프로젝트에 환경 변수 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 포함되어 있지 않은지 확인합니다. 프로젝트 환경 변수에 일반 텍스트 자격 증명이 포함된 경우, 이 규칙은 NON_COMPLIANT로 간주됩니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Amazon EKS 클러스터가 KMS를 사용하여 암호화된 AWS Kubernetes 보안 암호를 갖도록 구성되지 않았는지 확인합니다. EKS 클러스터에 encryptionConfig 리소스가 없거나 encryptionConfig이 리소스를 보안 키로 명명하지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Amazon Kinesis 스트림이 서버 측 암호화를 사용하여 저장 시 암호화되는지 확인합니다. 'StreamEncryption'이 없는 경우 Kinesis 스트림의 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK 클러스터가 클러스터의 브로커 노드와 함께 HTTPS(TLS)를 사용하여 전송 중 암호화를 적용하는지 확인합니다. 클러스터 내 브로커 노드 연결에 대해 일반 텍스트 통신이 활성화된 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-encrypted	Amazon Neptune DB 클러스터에 스토리지 암호화가 활성화되어 있는지 확인합니다. 스토리지 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service(AWS DMS) 엔드포인트가 SSL 연결로 구성되어 있는지 확인합니다. AWS DMS에 SSL 연결이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
8.3.5	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	access-keys-rotated	유효한 IAM 액세스 키가 maxAccessKeyAge에 지정된 일수에 따라 교체(변경)되는지 확인합니다. 지정된 기간 내에 액세스 키가 교체되지 않는 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.5	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.5	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.3.7	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	access-keys-rotated	유효한 IAM 액세스 키가 maxAccessKeyAge에 지정된 일수에 따라 교체(변경)되는지 확인합니다. 지정된 기간 내에 액세스 키가 교체되지 않는 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.7	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.7	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.3.9	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	access-keys-rotated	유효한 IAM 액세스 키가 maxAccessKeyAge에 지정된 일수에 따라 교체(변경)되는지 확인합니다. 지정된 기간 내에 액세스 키가 교체되지 않는 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.9	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.9	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.4.1	CDE에 대한 액세스를 보호하기 위해 다중 인증(MFA)이 구현됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.4.2	CDE에 대한 액세스를 보호하기 위해 다중 인증(MFA)이 구현됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.4.3	CDE에 대한 액세스를 보호하기 위해 다중 인증(MFA)이 구현됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.6.3	애플리케이션 및 시스템 계정과 관련 인증 요소의 사용은 엄격하게 관리됩니다. (PCI-DSS-v4.0)	access-keys-rotated	유효한 IAM 액세스 키가 maxAccessKeyAge에 지정된 일수에 따라 교체(변경)되는지 확인합니다. 지정된 기간 내에 액세스 키가 교체되지 않는 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.6.3	애플리케이션 및 시스템 계정과 관련 인증 요소의 사용은 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.6.3	애플리케이션 및 시스템 계정과 관련 인증 요소의 사용은 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 수동 DB 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. 기존 및 신규 Neptune 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙은 웹 ACL과 연결되지 않은 경우 AWS AppSync API에 대한 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT 입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration 이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition 에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
A1.2.3	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	security-account-information-provided	AWS 계정 연락처에 대한 보안 연락처 정보를 제공했는지 확인합니다. 계정 내에 보안 연락처 정보가 제공되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.2.5.1	PCI DSS 범위는 문서화되고 검증됩니다. (PCI-DSS-v4.0)	macie-auto-sensitive-data-discovery-check	Amazon Macie 에 민감한 데이터 자동 검색이 활성화되어 있는지 확인합니다. 민감한 데이터 자동 검색이 비활성화된 경우 규칙은 NON_COMPLIANT입니다. 이 규칙은 관리자 계정에는 APPLICABLE, 구성원 계정에는 NOT_APPLICABLE입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.2.5.1	PCI DSS 범위는 문서화되고 검증됩니다. (PCI-DSS-v4.0)	macie-status-check	리전별 계정에서 Amazon Macie가 활성화되어 있는지 확인합니다. 'status' 속성이 'ENABLED'로 설정되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.2.5.2	PCI DSS 범위는 문서화되고 검증됩니다. (PCI-DSS-v4.0)	macie-auto-sensitive-data-discovery-check	Amazon Macie 에 민감한 데이터 자동 검색이 활성화되어 있는지 확인합니다. 민감한 데이터 자동 검색이 비활성화된 경우 규칙은 NON_COMPLIANT입니다. 이 규칙은 관리자 계정에는 APPLICABLE, 구성원 계정에는 NOT_APPLICABLE입니다.
A3.2.5.2	PCI DSS 범위는 문서화되고 검증됩니다. (PCI-DSS-v4.0)	macie-status-check	리전별 계정에서 Amazon Macie가 활성화되어 있는지 확인합니다. 'status' 속성이 'ENABLED'로 설정되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	지정된 지표 이름의 CloudWatch 경보 설정이 지정한 설정과 일치하는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 수동 DB 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. 기존 및 신규 Neptune 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-secret-unused	지정된 일수 내에 AWS Secrets Manager 보안 암호에 액세스했는지 확인합니다. 'unusedForDays' 일수 내에 보안 암호에 액세스하지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT 입니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	지정된 지표 이름의 CloudWatch 경보 설정이 지정한 설정과 일치하는지 확인합니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

템플릿

템플릿은 GitHub: PCI DSS 4.0(글로벌 리소스 유형 제외) 운영 모범 사례에서 확인할 수 있습니다.

PCI DSS 4.0 운영 모범 사례(글로벌 리소스 유형 포함)

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Payment Card Industry Data Security Standard(PCI DSS) 4.0(글로벌 리소스 유형 제외)과 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 AWS Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 PCI DSS 제어와 관련이 있습니다. PCI DSS 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.5	네트워크 보안 제어(NSC)를 구성하고 유	cloudfront-security-policy-check	Amazon CloudFront 배포가 시청자 연결에 대해 최소 보안 정

제어 ID	제어 설명	AWS 구성 규칙	지침
	지 관리합니다. (PCI-DSS-v4.0)		책 및 TLSv1.2 이상의 암호 그룹을 사용하고 있는지 확인합니다. minimumProtocolVersion이 TLSv1.2_2018 이하이면 CloudFront 배포의 경우 이 규칙은 NON_COMPLIANT입니다.
1.2.5	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	cloudfront-sni-enabled	Amazon CloudFront 배포가 사용자 지정 SSL 인증서를 사용하고 있으며 SNI를 사용하여 HTTPS 요청을 처리하도록 구성되어 있는지 확인합니다. 사용자 지정 SSL 인증서가 연결되어 있지만 SSL 지원 메서드가 전용 IP 주소인 경우 규칙은 NON_COMPLIANT입니다.
1.2.5	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	AWS Transfer Family로 생성된 서버가 엔드포인트 연결에 FTP를 사용하지 않는지 확인합니다. 엔드포인트 연결을 위한 서버 프로토콜이 FTP를 활성화한 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.5	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront 배포가 CloudFront 엣지 로케이션과 사용자 지정 오리진 간의 HTTPS 통신에 더 이상 사용되지 않는 SSL 프로토콜을 사용하고 있지 않는지 확인합니다. 'OriginSslProtocols'에 'SSLv3'이 포함된 경우 이 규칙은 CloudFront 배포에 대해 NON_COMPLIANT입니다.
1.2.5	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront 배포가 사용자 지정 오리진에 대한 트래픽을 암호화하고 있는지 확인합니다. 'OriginProtocolPolicy'가 'http-only' 또는 'OriginProtocolPolicy'가 'match-viewer'이고 'ViewerProtocolPolicy'가 'allow-all'인 경우, 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.5	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront 배포에서 HTTPS(직접 또는 리디렉션)를 사용하는지 확인합니다. ViewerProtocolPolicy의 값이 DefaultCacheBehavior 또는 CacheBehaviors에 대해 'allow-all'로 설정되어 있으면 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront 배포가 웹 애플리케이션 방화벽(WAF) 또는 WAFv2 웹 액세스 제어 목록(ACL)과 연결되어 있는지 확인합니다. CloudFront 배포가 WAF 웹 ACL과 연결되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service(Amazon RDS) DB 보안 그룹이 기본 그룹인지 확인합니다. 기본 DB 보안 그룹이 아닌 DB 보안 그룹이 있는 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud(Amazon EC2) Tranit Gateways에 'AutoAcceptSharedAttachments'가 활성화되어 있지 않았는지 확인합니다. 'AutoAcceptSharedAttachments'가 '활성화'로 설정된 경우 Transit Gateway의 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙은 웹 ACL과 연결되지 않은 경우 AWS AppSync API에 대한 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global Web ACL에 일부 WAF 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic 규칙 그룹에 몇 가지 규칙이 포함되어 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF 글로벌 규칙에 몇 가지 조건이 포함되어 있는지 확인합니다. WAF 글로벌 규칙 내에 조건이 없는 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.2.8	네트워크 보안 제어(NSC)를 구성하고 유지 관리합니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront 배포가 웹 애플리케이션 방화벽(WAF) 또는 WAFv2 웹 액세스 제어 목록(ACL)과 연결되어 있는지 확인합니다. CloudFront 배포가 WAF 웹 ACL과 연결되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service(Amazon RDS) DB 보안 그룹이 기본 그룹인지 확인합니다. 기본 DB 보안 그룹이 아닌 DB 보안 그룹이 있는 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift 클러스터에 'enhanced VpcRouting'이 활성화되어 있는지 확인합니다. 'enhanced VpcRouting'이 활성화되지 않았거나, configuration.enhancedVpcRouting 필드가 'false'인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud(Amazon EC2) Tranit Gateways에 'AutoAcceptSharedAttachments'가 활성화되어 있지 않았는지 확인합니다. 'AutoAcceptSharedAttachments'가 '활성화'로 설정된 경우 Transit Gateway의 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙은 웹 ACL과 연결되지 않은 경우 AWS AppSync API에 대한 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global Web ACL에 일부 WAF 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic 규칙 그룹에 몇 가지 규칙이 포함되어 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF 글로벌 규칙에 몇 가지 조건이 포함되어 있는지 확인합니다. WAF 글로벌 규칙 내에 조건이 없는 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.3.1	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront 배포가 웹 애플리케이션 방화벽(WAF) 또는 WAFv2 웹 액세스 제어 목록(ACL)과 연결되어 있는지 확인합니다. CloudFront 배포가 WAF 웹 ACL과 연결되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service(Amazon RDS) DB 보안 그룹이 기본 그룹인지 확인합니다. 기본 DB 보안 그룹이 아닌 DB 보안 그룹이 있는 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift 클러스터에 'enhanced VpcRouting'이 활성화되어 있는지 확인합니다. 'enhanced VpcRouting'이 활성화되지 않았거나, configuration.enhancedVpcRouting 필드가 'false'인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud(Amazon EC2) Tranit Gateways에 'AutoAcceptSharedAttachments'가 활성화되어 있지 않았는지 확인합니다. 'AutoAcceptSharedAttachments'가 '활성화'로 설정된 경우 Transit Gateway의 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙은 웹 ACL과 연결되지 않은 경우 AWS AppSync API에 대한 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global Web ACL에 일부 WAF 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic 규칙 그룹에 몇 가지 규칙이 포함되어 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF 글로벌 규칙에 몇 가지 조건이 포함되어 있는지 확인합니다. WAF 글로벌 규칙 내에 조건이 없는 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.3.2	카드 소지자 데이터 환경에 대한 네트워크 액세스는 제한됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
1.4.1	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.1	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift 클러스터에 'enhancedVpcRouting'이 활성화되어 있는지 확인합니다. 'enhancedVpcRouting'이 활성화되지 않았거나, configuration.enhancedVpcRouting 필드가 'false'인 경우 규칙은 NON_COMPLIANT입니다.
1.4.1	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront 배포가 웹 애플리케이션 방화벽(WAF) 또는 WAFv2 웹 액세스 제어 목록(ACL)과 연결되어 있는지 확인합니다. CloudFront 배포가 WAF 웹 ACL과 연결되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service(Amazon RDS) DB 보안 그룹이 기본 그룹인지 확인합니다. 기본 DB 보안 그룹이 아닌 DB 보안 그룹이 있는 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift 클러스터에 'enhanced VpcRouting'이 활성화되어 있는지 확인합니다. 'enhanced VpcRouting'이 활성화되지 않았거나, configuration.enhancedVpcRouting 필드가 'false'인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud(Amazon EC2) Tranit Gateways에 'AutoAcceptSharedAttachments'가 활성화되어 있지 않았는지 확인합니다. 'AutoAcceptSharedAttachments'가 '활성화'로 설정된 경우 Transit Gateway의 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙은 웹 ACL과 연결되지 않은 경우 AWS AppSync API에 대한 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global Web ACL에 일부 WAF 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic 규칙 그룹에 몇 가지 규칙이 포함되어 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF 글로벌 규칙에 몇 가지 조건이 포함되어 있는지 확인합니다. WAF 글로벌 규칙 내에 조건이 없는 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.4.2	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
1.4.3	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.3	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.
1.4.3	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-full-packets	AWS Network Firewall 정책이 전체 패킷에 대해 사용자 정의 기본 상태 비저장 작업으로 구성되어 있는지 확인합니다. 전체 기본 상태 비저장 작업이 사용자 정의 기본 상태 비저장 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.4	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.
1.4.4	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-enabled	Amazon Redshift 클러스터에 'enhancedVpcRouting'이 활성화되어 있는지 확인합니다. 'enhancedVpcRouting'이 활성화되지 않았거나, configuration.enhancedVpcRouting 필드가 'false'인 경우 규칙은 NON_COMPLIANT입니다.
1.4.4	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.4.5	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	ecs-task-definition-pid-mode-check	ECSTaskDefinitions가 호스트의 프로세스 네임스페이스를 Amazon Elastic Container Service(Amazon ECS) 컨테이너와 공유하도록 구성되어 있는지 확인합니다. pidMode 파라미터가 'host'로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.4.5	신뢰할 수 있는 네트워크와 신뢰할 수 없는 네트워크 간의 네트워크 연결을 제어합니다. (PCI-DSS-v4.0)	ec2-launch-template-public-ip-disabled	Amazon EC2 시작 템플릿이 네트워크 인터페이스에 퍼블릭 IP 주소를 할당하도록 설정되지 않았는지 확인합니다. EC2 시작 템플릿의 기본 버전에 'AssociatePublicIpAddress'가 'true'로 설정된 네트워크 인터페이스가 하나 이상 있는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront 배포가 웹 애플리케이션 방화벽(WAF) 또는 WAFv2 웹 액세스 제어 목록(ACL)과 연결되어 있는지 확인합니다. CloudFront 배포가 WAF 웹 ACL과 연결되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service(Amazon RDS) DB 보안 그룹이 기본 그룹인지 확인합니다. 기본 DB 보안 그룹이 아닌 DB 보안 그룹이 있는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud(Amazon EC2) Tranit Gateways에 'AutoAcceptSharedAttachments'가 활성화되어 있지 않았는지 확인합니다. 'AutoAcceptSharedAttachments'가 '활성화'로 설정된 경우 Transit Gateway의 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙은 웹 ACL과 연결되지 않은 경우 AWS AppSync API에 대한 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global Web ACL에 일부 WAF 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic 규칙 그룹에 몇 가지 규칙이 포함되어 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF 글로벌 규칙에 몇 가지 조건이 포함되어 있는지 확인합니다. WAF 글로벌 규칙 내에 조건이 없는 경우 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
1.5.1	신뢰할 수 없는 네트워크와 CDE 모두에 연결할 수 있는 컴퓨팅 디바이스로 인한 CDE의 위험이 완화됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
10.2.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT 입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.1	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.3	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.4	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.5	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.6	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
10.2.1.7	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT 입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
10.2.2	감사 로그는 비정상 및 의심스러운 활동의 탐지와 이벤트에 대한 포렌식 분석을 지원하기 위해 구현됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT 입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT 입니다.
10.3.1	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT 입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 수동 DB 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. 기존 및 신규 Neptune 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
10.3.2	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	aurora-resources-protected-by-backup-plan	Amazon Aurora DB 클러스터가 백업 계획으로 보호되고 있는지 확인합니다. Amazon Relational Database Service(RDS) 데이터베이스 클러스터가 백업 계획에 의해 보호되고 있지 않을 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	db-instance-backup-enabled	RDS DB 인스턴스에 백업이 활성화되어 있는지 확인합니다. 이 규칙은 필요에 따라 백업 보존 기간과 백업 기간을 확인합니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	dynamodb-in-backup-plan	Amazon DynamoDB 테이블이 AWS 백업 계획에 있는지 확인합니다. Amazon DynamoDB 테이블이 AWS 백업 계획에 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	dynamodb-resources-protected-by-backup-plan	Amazon DynamoDB 테이블이 백업 계획으로 보호되는지 확인합니다. DynamoDB 테이블을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT 입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	ebs-in-backup-plan	AWS 백업의 백업 계획에 Amazon Elastic Block Store(Amazon EBS) 볼륨이 추가되었는지 확인합니다. Amazon EBS 볼륨이 백업 계획에 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	ebs-resources-protected-by-backup-plan	Amazon Elastic Block Store(Amazon EBS) 볼륨이 백업 계획으로 보호되는지 확인합니다. Amazon EBS 볼륨을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	ec2-resources-protected-by-backup-plan	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스가 백업 계획으로 보호되는지 확인합니다. Amazon EC2 인스턴스를 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	efs-in-backup-plan	AWS 백업의 백업 계획에 Amazon Elastic File System(Amazon EFS) 파일 시스템이 추가되었는지 확인합니다. EFS 파일 시스템이 백업 계획에 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	efs-resources-protected-by-backup-plan	Amazon Elastic File System(Amazon EFS) 파일 시스템이 백업 계획으로 보호되는지 확인합니다. EFS 파일 시스템을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	elasticache-redis-cluster-automatic-backup-check	Amazon ElastiCache Redis 클러스터에 자동 백업이 설정되어 있는지 확인합니다. Redis 클러스터에 대한 SnapshotRetentionLimit가 SnapshotRetentionPeriod 파라미터보다 작으면 규칙은 NON_COMPLIANT입니다. 예를 들어 파라미터가 15인 경우 snapshotRetentionPeriod가 0~15이면 규칙이 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	fsx-resources-protected-by-backup-plan	Amazon FSx 파일 시스템이 백업 계획에 의해 보호되고 있는지 확인합니다. Amazon FSx 파일 시스템을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-backup-retention-check	Amazon Neptune DB 클러스터 보존 기간이 특정 일수로 설정되어 있는지 확인합니다. 보존 기간이 파라미터에서 지정된 값보다 짧은 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	rds-in-backup-plan	Amazon Relational Database Service(Amazon RDS) 데이터베이스가 AWS 백업 계획에 있는지 확인합니다. Amazon RDS 데이터베이스가 AWS 백업 계획에 포함되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	rds-resources-protected-by-backup-plan	Amazon Relational Database Service(Amazon RDS) 인스턴스가 백업 계획으로 보호되는지 확인합니다. Amazon RDS 인스턴스를 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	redshift-backup-enabled	클러스터에 대해 Amazon Redshift 자동 스냅샷이 활성화되어 있는지 확인합니다. automatedSnapshotRetentionPeriod의 값이 MaxRetentionPeriod보다 크거나 MinRetentionPeriod보다 작거나 값이 0인 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-resources-protected-by-backup-plan	Amazon Simple Storage Service(Amazon S3) 버킷이 백업 플랜에 의해 보호되는지 확인합니다. Amazon S3 버킷을 백업 계획에서 지원하지 않는 경우 규칙은 NON_COMPLIANT입니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	db-instance-backup-enabled	RDS DB 인스턴스에 백업이 활성화되어 있는지 확인합니다. 이 규칙은 필요에 따라 백업 보존 기간과 백업 기간을 확인합니다.
10.3.3	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.4	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudfront-origin-access-identity-enabled	Amazon S3 오리진 유형을 사용하는 CloudFront 배포에 오리진 액세스 ID(OAI)가 구성되어 있는지 확인합니다. CloudFront 배포가 S3에 의해 지원되고 모든 오리진 유형이 OAI로 구성되어 있지 않거나, 오리진이 S3 버킷이 아닌 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.4	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudfront-s3-origin-access-control-enabled	Amazon Simple Storage Service(Amazon S3) 오리진 유형을 사용하는 Amazon CloudFront 배포에 원본 액세스 제어(OAC)가 활성화되어 있는지 확인합니다. OAC가 활성화되지 않은 Amazon S3 오리진을 사용하는 CloudFront 배포의 경우 이 규칙은 NON_COMPLIANT입니다.
10.3.4	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-bucket-default-lock-enabled	기본적으로 S3 버킷에 잠금이 활성화되어 있는지 확인합니다. 잠금이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.3.4	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	s3-bucket-versioning-enabled	S3 버킷에 버전 관리가 활성화되어 있는지 확인합니다. 이 규칙은 필요에 따라 S3 버킷에 MFA 삭제가 활성화되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.3.4	감사 로그는 파기 및 무단 수정으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT 입니다.
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT 입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.
10.4.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig. CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.
10.4.1.1	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.
10.4.2	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.4.3	감사 로그를 검토하여 비정상 또는 의심스러운 활동을 식별합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.5.1	감사 로그 기록은 유지되며 분석에 사용할 수 있습니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT입니다.
10.5.1	감사 로그 기록은 유지되며 분석에 사용할 수 있습니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.5.1	감사 로그 기록은 유지되며 분석에 사용할 수 있습니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.5.1	감사 로그 기록은 유지되며 분석에 사용할 수 있습니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.5.1	감사 로그 기록은 유지되며 분석에 사용할 수 있습니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.6.3	시간 동기화 메커니즘은 모든 시스템에서 일관된 시간 설정을 지원합니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation 스택이 Amazon SNS 주제로 이벤트 알림을 전송하는지 확인합니다. 필요한 경우 특정 Amazon SNS 주제가 사용되는지 여부를 확인합니다. CloudFormation 스택이 알림을 전송하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.
10.7.1	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation 스택이 Amazon SNS 주제로 이벤트 알림을 전송하는지 확인합니다. 필요한 경우 특정 Amazon SNS 주제가 사용되는지 여부를 확인합니다. CloudFormation 스택이 알림을 전송하지 않는 경우 규칙은 NON_COMPLIANT입니다.
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT 입니다.
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig. CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
10.7.2	중요한 보안 제어 시스템의 장애를 즉시 감지, 보고 및 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
11.5.2	네트워크 침입 및 예기치 않은 파일 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation 스택이 Amazon SNS 주제로 이벤트 알림을 전송하는지 확인합니다. 필요한 경우 특정 Amazon SNS 주제가 사용되는지 여부를 확인합니다. CloudFormation 스택이 알림을 전송하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.5.2	네트워크 침입 및 예기치 않은 파일 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
11.5.2	네트워크 침입 및 예기치 않은 파일 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
11.5.2	네트워크 침입 및 예기치 않은 파일 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	지정된 지표 이름의 CloudWatch 경보 설정이 지정한 설정과 일치하는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.5.2	네트워크 침입 및 예기치 않은 파일 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
11.6.1	결제 페이지의 무단 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation 스택이 Amazon SNS 주제로 이벤트 알림을 전송하는지 확인합니다. 필요한 경우 특정 Amazon SNS 주제가 사용되는지 여부를 확인합니다. CloudFormation 스택이 알림을 전송하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.6.1	결제 페이지의 무단 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
11.6.1	결제 페이지의 무단 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
11.6.1	결제 페이지의 무단 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	지정된 지표 이름의 CloudWatch 경보 설정이 지정한 설정과 일치하는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
11.6.1	결제 페이지의 무단 변경 사항을 감지하고 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
12.10.5	CDE에 영향을 미칠 수 있는 의심되고 확인된 보안 사고에 즉시 대응합니다. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation 스택이 Amazon SNS 주제로 이벤트 알림을 전송하는지 확인합니다. 필요한 경우 특정 Amazon SNS 주제가 사용되는지 여부를 확인합니다. CloudFormation 스택이 알림을 전송하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.10.5	CDE에 영향을 미칠 수 있는 의심되고 확인된 보안 사고에 즉시 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
12.10.5	CDE에 영향을 미칠 수 있는 의심되고 확인된 보안 사고에 즉시 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
12.10.5	CDE에 영향을 미칠 수 있는 의심되고 확인된 보안 사고에 즉시 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	지정된 지표 이름의 CloudWatch 경보 설정이 지정한 설정과 일치하는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
12.10.5	CDE에 영향을 미칠 수 있는 의심되고 확인된 보안 사고에 즉시 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
12.4.2.1	PCI DSS 규정 준수를 관리합니다. (PCI-DSS-v4.0)	service-catalog-shared-within-organization	AWS Organizations와의 통합이 활성화된 경우 AWS Service Catalog가 조직(단일 단위로 취급되는 AWS 계정 모음)과 포트폴리오를 공유하는지 확인합니다. 공유의 `Type` 값이 `ACCOUNT`인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.5	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	cloudfront-security-policy-check	Amazon CloudFront 배포가 시청자 연결에 대해 최소 보안 정책 및 TLSv1.2 이상의 암호 그룹을 사용하고 있는지 확인합니다. minimumProtocolVersion이 TLSv1.2_2018 이하이면 CloudFront 배포의 경우 이 규칙은 NON_COMPLIANT입니다.
2.2.5	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	cloudfront-sni-enabled	Amazon CloudFront 배포가 사용자 지정 SSL 인증서를 사용하고 있으며 SNI를 사용하여 HTTPS 요청을 처리하도록 구성되어 있는지 확인합니다. 사용자 지정 SSL 인증서가 연결되어 있지만 SSL 지원 메서드가 전용 IP 주소인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.5	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	AWS Transfer Family로 생성된 서버가 엔드포인트 연결에 FTP를 사용하지 않는지 확인합니다. 엔드포인트 연결을 위한 서버 프로토콜이 FTP를 활성화한 경우 규칙은 NON_COMPLIANT입니다.
2.2.5	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront 배포가 CloudFront 엣지 로케이션과 사용자 지정 오리진 간의 HTTPS 통신에 더 이상 사용되지 않는 SSL 프로토콜을 사용하고 있지 않는지 확인합니다. 'OriginSslProtocols'에 'SSLv3'이 포함된 경우 이 규칙은 CloudFront 배포에 대해 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.5	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront 배포가 사용자 지정 오리진에 대한 트래픽을 암호화하고 있는지 확인합니다. 'OriginProtocolPolicy'가 'http-only' 또는 'OriginProtocolPolicy'가 'match-viewer'이고 'ViewerProtocolPolicy'가 'allow-all'인 경우, 규칙은 NON_COMPLIANT입니다.
2.2.5	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront 배포에서 HTTPS(직접 또는 리디렉션)를 사용하는지 확인합니다. ViewerProtocolPolicy의 값이 DefaultCacheBehavior 또는 CacheBehaviors에 대해 'allow-all'로 설정되어 있으면 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis 데이터 스토어용 AWS 데이터베이스 마이그레이션 서비스(AWS DMS) 엔드포인트가 다른 엔드포인트와 통신하는 데이터의 TLS/SSL 암호화에 활성화되어 있는지 확인합니다. TLS/SSL 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront 배포가 CloudFront 엣지 로케이션과 사용자 지정 오리진 간의 HTTPS 통신에 더 이상 사용되지 않는 SSL 프로토콜을 사용하고 있지 않는지 확인합니다. 'OriginSslProtocols'에 'SSLv3'이 포함된 경우 이 규칙은 CloudFront 배포에 대해 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront 배포가 사용자 지정 오리진에 대한 트래픽을 암호화하고 있는지 확인합니다. 'OriginProtocolPolicy'가 'http-only' 또는 'OriginProtocolPolicy'가 'match-viewer'이고 'ViewerProtocolPolicy'가 'allow-all'인 경우, 규칙은 NON_COMPLIANT입니다.
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront 배포에서 HTTPS(직접 또는 리디렉션)를 사용하는지 확인합니다. ViewerProtocolPolicy의 값이 DefaultCacheBehavior 또는 CacheBehaviors에 대해 'allow-all'로 설정되어 있으면 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Amazon DynamoDB Accelerator(DAX) 클러스터에 ClusterEndpointEncryptionType이 TLS로 설정되어 있는지 확인합니다. DAX 클러스터가 Transport Layer Security(TLS)로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK 클러스터가 클러스터의 브로커 노드와 함께 HTTPS(TLS)를 사용하여 전송 중 암호화를 적용하는지 확인합니다. 클러스터 내 브로커 노드 연결에 대해 일반 텍스트 통신이 활성화된 경우 규칙은 NON_COMPLIANT입니다.
2.2.7	시스템 구성 요소를 안전하게 구성하고 관리합니다. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS 데이터베이스 마이그레이션 서비스(AWS DMS) 엔드포인트가 SSL 연결로 구성되어 있는지 확인합니다. AWS DMS에 SSL 연결이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.2.1	계정 데이터의 저장은 최소한으로 유지됩니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.2.1	계정 데이터의 저장은 최소한으로 유지됩니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.
3.2.1	계정 데이터의 저장은 최소한으로 유지됩니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.2.1	계정 데이터의 저장은 최소한으로 유지됩니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1.1	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.
3.3.1.1	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.
3.3.1.1	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1.1	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.
3.3.1.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.
3.3.1.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.1.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.3.1.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.
3.3.2	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.2	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.
3.3.2	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.3.2	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ec2-volume-inuse-check	EBS 볼륨이 EC2 인스턴스에 연결되어 있는지 확인합니다. 필요한 경우, 인스턴스 종료 시 EBS 볼륨이 삭제 대기 상태가 되는지 확인합니다.
3.3.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-configured	프라이빗 Amazon Elastic Container Registry(ECR) 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 프라이빗 리포지토리에 대해 구성된 수명 주기 정책이 없는 경우 규칙은 NON_COMPLIANT입니다.
3.3.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Amazon DynamoDB 테이블에 대해 시점 복구(PITR)가 활성화되어 있는지 확인합니다. PITR이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3.3	민감한 인증 데이터(SAD)는 권한 부여 후 저장되지 않습니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-rest	Amazon Athena 작업 그룹이 저장 시 암호화되는지 확인합니다. Athena 작업 그룹에 대해 저장 데이터 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Amazon Neptune DB 클러스터에 암호화된 스냅샷이 있는지 확인합니다. Neptune 클러스터에 암호화된 스냅샷이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Amazon Redshift 클러스터가 암호화에 지정된 AWS Key Management Service(AWS KMS) 키를 사용하고 있는지 확인합니다. 암호화가 활성화되어 있고 kmsKeyArn 파라미터에 제공된 키로 클러스터가 암호화된 경우 규칙은 COMPLIANT입니다. 클러스터가 암호화되지 않거나 다른 키로 암호화된 경우 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	codebuild-project-artifact-encryption	AWS CodeBuild 프로젝트에 모든 아티팩트에 대해 암호화가 활성화되어 있는지 확인합니다. 기본 또는 보조(있는 경우) 아티팩트 구성에 대해 'encryptionDisabled'가 'true'로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	codebuild-project-s3-logs-encrypted	Amazon S3 Logs로 구성된 AWS CodeBuild 프로젝트에 해당 로그에 암호화가 활성화되어 있는지 확인합니다. CodeBuild 프로젝트의 S3LogsConfig에서 'encryptionDisabled'가 'true'로 설정된 경우 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	dax-encryption-enabled	Amazon DynamoDB Accelerator(DAX) 클러스터가 암호화되어 있는지 확인합니다. DAX 클러스터가 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	eks-secrets-encrypted	Amazon Elastic Kubernetes Service 클러스터가 AWS Key Management Service(KMS) 키를 사용하여 Kubernetes 보안 암호를 암호화하도록 구성되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	api-gw-cache-enabled-and-encrypted	Amazon API Gateway 단계의 모든 메서드에 캐시가 활성화되어 있고 캐시가 암호화되어 있는지 확인합니다. Amazon API Gateway 단계에 캐싱이 구성되지 않았거나, 캐시가 암호화되지 않은 메서드가 있을 경우 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	docdb-cluster-encrypted	Amazon DocumentDB(MongoDB 호환) 클러스터에 대해 스토리지 암호화가 활성화되어 있는지 확인합니다. 스토리지 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블이 AWS Key Management Service(KMS)로 암호화되어 있는지 확인합니다. Amazon DynamoDB 테이블이 AWS KMS로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다. 암호화된 AWS KMS 키가 kmsKeyArns 입력 파라미터에 없는 경우에도 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	dynamodb-table-encryption-enabled	Amazon DynamoDB 테이블이 암호화되어 있는지 확인하고 상태를 확인합니다. 상태가 활성화되었거나 활성화 중인 경우 규칙이 COMPLIANT로 간주됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	프로젝트에 환경 변수 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 포함되어 있지 않은지 확인합니다. 프로젝트 환경 변수에 일반 텍스트 자격 증명이 포함된 경우, 이 규칙은 NON_COMPLIANT로 간주됩니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Amazon EKS 클러스터가 KMS를 사용하여 암호화된 AWS Kubernetes 보안 암호를 갖도록 구성되지 않았는지 확인합니다. EKS 클러스터에 encryptionConfig 리소스가 없거나 encryptionConfig이 리소스를 보안 키로 명명하지 않은 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Amazon Kinesis 스트림이 서버 측 암호화를 사용하여 저장 시 암호화되는지 확인합니다. 'StreamEncryption'이 없는 경우 Kinesis 스트림의 규칙은 NON_COMPLIANT입니다.
3.5.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-encrypted	Amazon Neptune DB 클러스터에 스토리지 암호화가 활성화되어 있는지 확인합니다. 스토리지 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.5.1.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
3.5.1.1	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 수동 DB 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. 기존 및 신규 Neptune 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
3.5.1.3	기본 계정 번호(PAN)는 저장된 모든 곳에서 보호됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.6.1	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
3.6.1.2	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1.2	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
3.6.1.2	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1.3	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.6.1.3	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1.3	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
3.6.1.4	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.6.1.4	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
3.6.1.4	저장된 계정 데이터를 보호하는 데 사용되는 암호화 키는 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.1	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-certificate-rsa-check	AWS Certificate Manager(ACM)에서 관리하는 RSA 인증서의 키 길이가 '2048'비트 이상인지 확인합니다. 최소 키 길이가 2048비트 미만인 경우 규칙은 NON_COMPLIANT입니다.
3.7.1	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.7.1	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.1	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
3.7.2	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.2	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
3.7.2	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.4	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.7.4	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.4	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
3.7.6	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.6	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
3.7.6	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.7	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
3.7.7	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.7.7	저장된 계정 데이터를 보호하기 위해 암호화를 사용하는 경우 키 수명 주기의 모든 측면을 다루는 키 관리 프로세스 및 절차가 정의되고 구현됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis 데이터 스토어용 AWS Database Migration Service(AWS DMS) 엔드포인트가 다른 엔드포인트와 통신하는 데이터의 TLS/SSL 암호화에 활성화되어 있는지 확인합니다. TLS/SSL 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront 배포가 CloudFront 엣지 로케이션과 사용자 지정 오리진 간의 HTTPS 통신에 더 이상 사용되지 않는 SSL 프로토콜을 사용하고 있지 않는지 확인합니다. 'OriginSslProtocols'에 'SSLv3'이 포함된 경우 이 규칙은 CloudFront 배포에 대해 NON_COMPLIANT입니다.
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront 배포가 사용자 지정 오리진에 대한 트래픽을 암호화하고 있는지 확인합니다. 'OriginProtocolPolicy'가 'http-only' 또는 'OriginProtocolPolicy'가 'match-viewer'이고 'ViewerProtocolPolicy'가 'allow-all'인 경우, 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront 배포에서 HTTPS(직접 또는 리디렉션)를 사용하는지 확인합니다. ViewerProtocolPolicy의 값이 DefaultCacheBehavior 또는 CacheBehaviors에 대해 'allow-all'로 설정되어 있으면 규칙은 NON_COMPLIANT입니다.
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Amazon DynamoDB Accelerator(DAX) 클러스터에 ClusterEndpointEncryptionType이 TLS로 설정되어 있는지 확인합니다. DAX 클러스터가 Transport Layer Security(TLS)로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK 클러스터가 클러스터의 브로커 노드와 함께 HTTPS(TLS)를 사용하여 전송 중 암호화를 적용하는지 확인합니다. 클러스터 내 브로커 노드 연결에 대해 일반 텍스트 통신이 활성화된 경우 규칙은 NON_COMPLIANT입니다.
4.2.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service(AWS DMS) 엔드포인트가 SSL 연결로 구성되어 있는지 확인합니다. AWS DMS에 SSL 연결이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	acm-pca-root-ca-disabled	AWS 프라이빗 인증 기관(AWS 프라이빗 CA)에 비활성화된 루트 CA가 있는지 확인합니다. 루트 CA의 상태가 DISABLED인 경우 규칙은 NON_COMPLIANT입니다.
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis 데이터 스토어용 AWS Database Migration Service(AWS DMS) 엔드포인트가 다른 엔드포인트와 통신하는 데이터의 TLS/SSL 암호화에 활성화되어 있는지 확인합니다. TLS/SSL 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront 배포가 CloudFront 엣지 로케이션과 사용자 지정 오리진 간의 HTTPS 통신에 더 이상 사용되지 않는 SSL 프로토콜을 사용하고 있지 않는지 확인합니다. 'OriginSslProtocols'에 'SSLv3'이 포함된 경우 이 규칙은 CloudFront 배포에 대해 NON_COMPLIANT입니다.
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront 배포가 사용자 지정 오리진에 대한 트래픽을 암호화하고 있는지 확인합니다. 'OriginProtocolPolicy'가 'http-only' 또는 'OriginProtocolPolicy'가 'match-viewer'이고 'ViewerProtocolPolicy'가 'allow-all'인 경우, 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront 배포에서 HTTPS(직접 또는 리디렉션)를 사용하는지 확인합니다. ViewerProtocolPolicy의 값이 DefaultCacheBehavior 또는 CacheBehaviors에 대해 'allow-all'로 설정되어 있으면 규칙은 NON_COMPLIANT입니다.
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Amazon DynamoDB Accelerator(DAX) 클러스터에 ClusterEndpointEncryptionType이 TLS로 설정되어 있는지 확인합니다. DAX 클러스터가 Transport Layer Security(TLS)로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK 클러스터가 클러스터의 브로커 노드와 함께 HTTPS(TLS)를 사용하여 전송 중 암호화를 적용하는지 확인합니다. 클러스터 내 브로커 노드 연결에 대해 일반 텍스트 통신이 활성화된 경우 규칙은 NON_COMPLIANT입니다.
4.2.1.1	PAN은 전송 중에 강력한 암호화로 보호됩니다. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service(AWS DMS) 엔드포인트가 SSL 연결로 구성되어 있는지 확인합니다. AWS DMS에 SSL 연결이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
5.3.4	맬웨어 방지 메커니즘 및 프로세스가 활성화, 유지 관리 및 모니터링됩니다. (PCI-DSS-v4.0)	cw-loggroup-retention-period-check	Amazon CloudWatch LogGroup 보존 기간이 365일을 초과하여 설정되어 있는지 또는 기타 지정된 보존 기간으로 설정되어 있는지 확인합니다. 보존 기간이 MinRetentionTime 보다 작거나 365일(지정된 경우)이면 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.3.3	보안 취약성을 식별하고 해결합니다. (PCI-DSS-v4.0)	lambda-function-settings-check	런타임, 역할, 제한 시간 및 메모리 크기에 대한 AWS Lambda 함수 설정이 예상 값과 일치하는지 확인합니다. 규칙은 '이미지' 패키지 유형이 있는 함수와 런타임이 'OS 전용 런타임'으로 설정된 함수를 무시합니다. Lambda 함수 설정이 예상 값과 일치하지 않는 경우 규칙은 NON_COMPLIANT입니다.
6.3.3	보안 취약성을 식별하고 해결합니다. (PCI-DSS-v4.0)	eks-cluster-oldest-supported-version	Amazon Elastic Kubernetes Service(EKS) 클러스터가 지원되는 가장 오래된 버전을 실행하고 있지 않는지 확인합니다. EKS 클러스터가 지원되는 가장 오래된 버전(파라미터 'oldestVersionSupported'와 같음)을 실행하는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4.1	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront 배포가 웹 애플리케이션 방화벽(WAF) 또는 WAFv2 웹 액세스 제어 목록(ACL)과 연결되어 있는지 확인합니다. CloudFront 배포가 WAF 웹 ACL과 연결되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
6.4.1	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙은 웹 ACL과 연결되지 않은 경우 AWS AppSync API에 대한 NON_COMPLIANT입니다.
6.4.1	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	wafv2-webacl-not-empty	WAFv2 리전 웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4.1	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	wafv2-rulegroup-not-empty	WAFv2 규칙 그룹에 규칙이 포함되어 있는지 확인합니다. WAFv2 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.
6.4.1	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global Web ACL에 일부 WAF 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
6.4.1	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic 규칙 그룹에 몇 가지 규칙이 포함되어 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.
6.4.1	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic 규칙 그룹에 몇 가지 규칙이 포함되어 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4.1	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF 글로벌 규칙에 몇 가지 조건이 포함되어 있는지 확인합니다. WAF 글로벌 규칙 내에 조건이 없는 경우 규칙은 NON_COMPLIANT입니다.
6.4.2	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront 배포가 웹 애플리케이션 방화벽(WAF) 또는 WAFv2 웹 액세스 제어 목록(ACL)과 연결되어 있는지 확인합니다. CloudFront 배포가 WAF 웹 ACL과 연결되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
6.4.2	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙이 웹 ACL과 연결되지 않은 경우 규칙은 AWS AppSync API에 대한 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4.2	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	wafv2-webacl-not-empty	WAFv2 리전 웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
6.4.2	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	wafv2-rulegroup-not-empty	WAFv2 규칙 그룹에 규칙이 포함되어 있는지 확인합니다. WAFv2 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.
6.4.2	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global Web ACL에 일부 WAF 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.4.2	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic 규칙 그룹에 몇 가지 규칙이 포함되어 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.
6.4.2	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic 규칙 그룹에 몇 가지 규칙이 포함되어 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.
6.4.2	퍼블릭 버전 웹 애플리케이션은 공격으로부터 보호됩니다. (PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF 글로벌 규칙에 몇 가지 조건이 포함되어 있는지 확인합니다. WAF 글로벌 규칙 내에 조건이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.5.5	모든 시스템 구성 요소에 대한 변경 사항을 안전하게 관리합니다. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-disabled	Lambda Compute Platform의 배포 그룹이 기본 배포 구성을 사용하지 않는지 확인합니다. 배포 그룹이 배포 구성 'CodeDeployDefault.LambdaAllAtOnce'를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
6.5.5	모든 시스템 구성 요소에 대한 변경 사항을 안전하게 관리합니다. (PCI-DSS-v4.0)	codepipeline-deployment-count-check	AWS CodePipeline의 첫 번째 배포 단계가 하나 이상의 배포를 수행하는지 확인합니다. 이는 지속적인 배포 활동을 모니터링하고, 정기적인 업데이트를 보장하며, 개발 또는 배포 프로세스에서 문제를 나타낼 수 있는 비활성 또는 활용도가 낮은 파이프라인을 식별하기 위한 것입니다. 필요한 경우, 각각의 이후 단계에서 지정된 배포 횟수(deploymentLimit) 이상을 배포하는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.5.6	모든 시스템 구성 요소에 대한 변경 사항을 안전하게 관리합니다. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-disabled	Lambda Compute Platform의 배포 그룹이 기본 배포 구성을 사용하지 않는지 확인합니다. 배포 그룹이 배포 구성 'CodeDeployDefault.LambdaAllAtOnce'를 사용하는 경우 규칙은 NON_COMPLIANT입니다.
6.5.6	모든 시스템 구성 요소에 대한 변경 사항을 안전하게 관리합니다. (PCI-DSS-v4.0)	codepipeline-deployment-count-check	AWS CodePipeline의 첫 번째 배포 단계가 하나 이상의 배포를 수행하는지 확인합니다. 이는 지속적인 배포 활동을 모니터링하고, 정기적인 업데이트를 보장하며, 개발 또는 배포 프로세스에서 문제를 나타낼 수 있는 비활성 또는 활용도가 낮은 파이프라인을 식별하기 위한 것입니다. 필요한 경우, 각각의 이후 단계에서 지정된 배포 횟수(deploymentLimit) 이상을 배포하는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대해 차단 목록에 있는 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	shield-drt-access	Shield 대응 팀(SRT)이 AWS 계정에 액세스할 수 있는지 확인합니다. AWS Shield Advanced가 활성화되어 있지만 SRT 액세스에 대한 역할이 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 클러스터에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 클러스터에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
7.2.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 인스턴스에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대해 차단 목록에 있는 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	shield-drt-access	Shield 대응 팀(SRT)이 AWS 계정에 액세스할 수 있는지 확인합니다. AWS Shield Advanced가 활성화되어 있지만 SRT 액세스에 대한 역할이 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 클러스터에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 클러스터에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
7.2.2	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 인스턴스에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.4	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	secretsmanager-secret-unused	지정된 일수 내에 AWS Secrets Manager 보안 암호에 액세스했는지 확인합니다. 'unusedForDays' 일수 내에 보안 암호에 액세스하지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대해 차단 목록에 있는 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	shield-drt-access	Shield 대응 팀(SRT)이 AWS 계정에 액세스할 수 있는지 확인합니다. AWS Shield Advanced가 활성화되어 있지만 SRT 액세스에 대한 역할이 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 클러스터에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 클러스터에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
7.2.5	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 인스턴스에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.5.1	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	secretsmanager-secret-unused	지정된 일수 내에 AWS Secrets Manager 보안 암호에 액세스했는지 확인합니다. 'unusedForDays' 일수 내에 보안 암호에 액세스하지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.2.6	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대해 차단 목록에 있는 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.2.6	시스템 구성 요소 및 데이터에 대한 액세스를 적절하게 정의하고 할당합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대해 차단 목록에 있는 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	shield-drt-access	Shield 대응 팀(SRT)이 AWS 계정에 액세스할 수 있는지 확인합니다. AWS Shield Advanced가 활성화되어 있지만 SRT 액세스에 대한 역할이 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 클러스터에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 클러스터에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
7.3.1	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 인스턴스에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대해 차단 목록에 있는 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	shield-drt-access	Shield 대응 팀(SRT)이 AWS 계정에 액세스할 수 있는지 확인합니다. AWS Shield Advanced가 활성화되어 있지만 SRT 액세스에 대한 역할이 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 클러스터에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 클러스터에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
7.3.2	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 인스턴스에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대해 차단 목록에 있는 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	shield-drt-access	Shield 대응 팀(SRT)이 AWS 계정에 액세스할 수 있는지 확인합니다. AWS Shield Advanced가 활성화되어 있지만 SRT 액세스에 대한 역할이 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 클러스터에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 클러스터에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
7.3.3	액세스 제어 시스템을 통해 시스템 구성 요소 및 데이터에 대한 액세스를 관리합니다. (PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 인스턴스에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.1	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.2.1	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud(EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되고 있지 않는지 확인합니다. 실행 중인 EC2 인스턴스가 키 페어를 사용하여 시작된 경우 규칙은 NON_COMPLIANT입니다.
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud(EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되고 있지 않는지 확인합니다. 실행 중인 EC2 인스턴스가 키 페어를 사용하여 시작된 경우 규칙은 NON_COMPLIANT입니다.
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	프로젝트에 환경 변수 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 포함되어 있지 않은지 확인합니다. 프로젝트 환경 변수에 일반 텍스트 자격 증명이 포함된 경우, 이 규칙은 NON_COMPLIANT로 간주됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.2	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-secret-unused	지정된 일수 내에 AWS Secrets Manager 보안 암호에 액세스했는지 확인합니다. 'unusedForDays' 일수 내에 보안 암호에 액세스하지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.2.4	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.2.4	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud(EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되고 있지 않는지 확인합니다. 실행 중인 EC2 인스턴스가 키 페어를 사용하여 시작된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.5	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.2.5	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud(EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되고 있지 않는지 확인합니다. 실행 중인 EC2 인스턴스가 키 페어를 사용하여 시작된 경우 규칙은 NON_COMPLIANT입니다.
8.2.6	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-secret-unused	지정된 일수 내에 AWS Secrets Manager 보안 암호에 액세스했는지 확인합니다. 'unusedForDays' 일수 내에 보안 암호에 액세스하지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	shield-drt-access	Shield 대응 팀(SRT)이 AWS 계정에 액세스할 수 있는지 확인합니다. AWS Shield Advanced가 활성화되어 있지만 SRT 액세스에 대한 역할이 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 클러스터에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 클러스터에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
8.2.7	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 인스턴스에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	shield-drt-access	Shield 대응 팀(SRT)이 AWS 계정에 액세스할 수 있는지 확인합니다. AWS Shield Advanced가 활성화되어 있지만 SRT 액세스에 대한 역할이 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 클러스터에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 클러스터에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터 버전이 인스턴스 메타데이터 서비스 버전2(IMDSv2)로 구성되었는지 확인합니다. HttpTokens가 선택 사항으로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	autoscaling-launchconfig-requires-imdsv2	IMDSv2만 활성화되어 있는지 확인합니다. 메타데이터 버전이 시작 구성에 포함되어 있지 않거나, 메타데이터 V1과 V2가 둘 다 활성화된 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
8.2.8	사용자 및 관리자의 사용자 식별 및 관련 계정은 계정 수명 주기 동안 엄격하게 관리됩니다. (PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 인스턴스에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.10.1	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	access-keys-rotated	유효한 IAM 액세스 키가 maxAccessKeyAge에 지정된 일수에 따라 교체(변경)되는지 확인합니다. 지정된 기간 내에 액세스 키가 교체되지 않는 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.3.10.1	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.10.1	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.11	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.3.11	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	ec2-no-amazon-key-pair	Amazon Elastic Compute Cloud(EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되고 있지 않는지 확인합니다. 실행 중인 EC2 인스턴스가 키 페어를 사용하여 시작된 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-rest	Amazon Athena 작업 그룹이 저장 시 암호화되는지 확인합니다. Athena 작업 그룹에 대해 저장 데이터 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Amazon Neptune DB 클러스터에 암호화된 스냅샷이 있는지 확인합니다. Neptune 클러스터에 암호화된 스냅샷이 없는 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Amazon Redshift 클러스터가 암호화에 지정된 AWS Key Management Service(AWS KMS) 키를 사용하고 있는지 확인합니다. 암호화가 활성화되어 있고 kmsKeyArn 파라미터에 제공된 키로 클러스터가 암호화된 경우 규칙은 COMPLIANT입니다. 클러스터가 암호화되지 않거나 다른 키로 암호화된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	codebuild-project-artifact-encryption	AWS CodeBuild 프로젝트에 모든 아티팩트에 대해 암호화가 활성화되어 있는지 확인합니다. 기본 또는 보조(있는 경우) 아티팩트 구성에 대해 'encryptionDisabled'가 'true'로 설정된 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	codebuild-project-s3-logs-encrypted	Amazon S3 Logs로 구성된 AWS CodeBuild 프로젝트에 해당 로그에 암호화가 활성화되어 있는지 확인합니다. CodeBuild 프로젝트의 S3LogsConfig에서 'encryptionDisabled'가 'true'로 설정된 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	dax-encryption-enabled	Amazon DynamoDB Accelerator(DAX) 클러스터가 암호화되어 있는지 확인합니다. DAX 클러스터가 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Redis 데이터 스토어용 AWS Database Migration Service(AWS DMS) 엔드포인트가 다른 엔드포인트와 통신하는 데이터의 TLS/SSL 암호화에 활성화되어 있는지 확인합니다. TLS/SSL 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	eks-secrets-encrypted	Amazon Elastic Kubernetes Service 클러스터가 AWS Key Management Service(KMS) 키를 사용하여 Kubernetes 보안 암호를 암호화하도록 구성되어 있는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	api-gw-cache-enabled-and-encrypted	Amazon API Gateway 단계의 모든 메서드에 캐시가 활성화되어 있고 캐시가 암호화되어 있는지 확인합니다. Amazon API Gateway 단계에 캐싱이 구성되지 않았거나, 캐시가 암호화되지 않은 메서드가 있을 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	docdb-cluster-encrypted	Amazon DocumentDB(MongoDB 호환) 클러스터에 대해 스토리지 암호화가 활성화되어 있는지 확인합니다. 스토리지 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블이 AWS Key Management Service(KMS)로 암호화되어 있는지 확인합니다. Amazon DynamoDB 테이블이 AWS KMS로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다. 암호화된 AWS KMS 키가 kmsKeyArns 입력 파라미터에 없는 경우에도 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	dynamodb-table-encryption-enabled	Amazon DynamoDB 테이블이 암호화되어 있는지 확인하고 상태를 확인합니다. 상태가 활성화되었거나 활성화 중인 경우 규칙이 COMPLIANT로 간주됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protocols	CloudFront 배포가 CloudFront 엣지 로케이션과 사용자 지정 오리진 간의 HTTPS 통신에 더 이상 사용되지 않는 SSL 프로토콜을 사용하고 있지 않는지 확인합니다. 'OriginSslProtocols'에 'SSLv3'이 포함된 경우 이 규칙은 CloudFront 배포에 대해 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-encrypted	Amazon CloudFront 배포가 사용자 지정 오리진에 대한 트래픽을 암호화하고 있는지 확인합니다. 'OriginProtocolPolicy'가 'http-only' 또는 'OriginProtocolPolicy'가 'match-viewer'이고 'ViewerProtocolPolicy'가 'allow-all'인 경우, 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Amazon CloudFront 배포에서 HTTPS(직접 또는 리디렉션)를 사용하는지 확인합니다. ViewerProtocolPolicy의 값이 DefaultCacheBehavior 또는 CacheBehaviors에 대해 'allow-all'로 설정되어 있으면 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-check	프로젝트에 환경 변수 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY가 포함되어 있지 않은지 확인합니다. 프로젝트 환경 변수에 일반 텍스트 자격 증명이 포함된 경우, 이 규칙은 NON_COMPLIANT로 간주됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Amazon DynamoDB Accelerator(DAX) 클러스터에 ClusterEndpointEncryptionType이 TLS로 설정되어 있는지 확인합니다. DAX 클러스터가 Transport Layer Security(TLS)로 암호화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Amazon EKS 클러스터가 KMS를 사용하여 암호화된 AWS Kubernetes 보안 암호를 갖도록 구성되지 않았는지 확인합니다. EKS 클러스터에 encryptionConfig 리소스가 없거나 encryptionConfig이 리소스를 보안 키로 명명하지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Amazon Kinesis 스트림이 서버 측 암호화를 사용하여 저장 시 암호화되는지 확인합니다. 'StreamEncryption'이 없는 경우 Kinesis 스트림의 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	msk-in-cluster-node-require-tls	Amazon MSK 클러스터가 클러스터의 브로커 노드와 함께 HTTPS(TLS)를 사용하여 전송 중 암호화를 적용하는지 확인합니다. 클러스터 내 브로커 노드 연결에 대해 일반 텍스트 통신이 활성화된 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-encrypted	Amazon Neptune DB 클러스터에 스토리지 암호화가 활성화되어 있는지 확인합니다. 스토리지 암호화가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.2	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	AWS Database Migration Service(AWS DMS) 엔드포인트가 SSL 연결로 구성되어 있는지 확인합니다. AWS DMS에 SSL 연결이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	s3-bucket-blacklisted-actions-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 버킷의 리소스에 대한 차단 목록 버킷 수준 및 객체 수준 작업을 허용하지 않는지 확인합니다. 예를 들어 규칙은 Amazon S3 버킷 정책이 버킷의 모든 객체에서 다른 AWS 계정이 s3:GetBucket* 작업 및 s3:DeleteObject를 수행하도록 허용하지 않는지 확인합니다. Amazon S3 버킷 정책에서 블랙리스트에 등록된 작업을 허용하는 경우 규칙이 NON_COMPLIANT로 간주됩니다.
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	s3-bucket-policy-not-more-permissive	Amazon Simple Storage Service(Amazon S3) 버킷 정책이 사용자가 제공하는 Amazon S3 버킷 정책을 제어하는 다른 계정 간 권한을 허용하지 않는지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	shield-drt-access	Shield 대응 팀(SRT)이 AWS 계정에 액세스할 수 있는지 확인합니다. AWS Shield Advanced가 활성화되어 있지만 SRT 액세스에 대한 역할이 구성되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	iam-policy-in-use	IAM 정책 ARN이 IAM 사용자 또는 한 명 이상의 IAM 사용자가 있는 그룹 또는 하나 이상의 신뢰할 수 있는 엔터티가 있는 IAM 역할에 연결되어 있는지 확인합니다.
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	neptune-cluster-iam-database-authentication	Amazon Neptune 클러스터에 AWS Identity and Access Management(IAM) 데이터베이스 인증이 활성화되어 있는지 확인합니다. Amazon Neptune 클러스터에 IAM 데이터베이스 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 클러스터에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 클러스터에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	ec2-instance-profile-attached	EC2 인스턴스에 AWS Identity and Access Management(IAM) 프로파일이 연결되어 있는지 확인합니다. EC2 인스턴스에 IAM 프로필이 연결되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
8.3.4	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	rds-instance-iam-authentication-enabled	Amazon Relational Database Service(Amazon RDS) 인스턴스에 AWS Identity and Access Management(IAM) 인증이 활성화되어 있는지 확인합니다. Amazon RDS 인스턴스에 IAM 인증이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.5	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	access-keys-rotated	유효한 IAM 액세스 키가 maxAccessKeyAge에 지정된 일수에 따라 교체(변경)되는지 확인합니다. 지정된 기간 내에 액세스 키가 교체되지 않는 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.3.5	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.5	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.7	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	access-keys-rotated	유효한 IAM 액세스 키가 maxAccessKeyAge에 지정된 일수에 따라 교체(변경)되는지 확인합니다. 지정된 기간 내에 액세스 키가 교체되지 않는 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.3.7	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.7	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.3.9	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	access-keys-rotated	유효한 IAM 액세스 키가 maxAccessKeyAge에 지정된 일수에 따라 교체(변경)되는지 확인합니다. 지정된 기간 내에 액세스 키가 교체되지 않는 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.3.9	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.3.9	사용자 및 관리자에 대한 강력한 인증을 설정하고 관리합니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.4.1	CDE에 대한 액세스를 보호하기 위해 다중 인증(MFA)이 구현됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.4.2	CDE에 대한 액세스를 보호하기 위해 다중 인증(MFA)이 구현됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.4.3	CDE에 대한 액세스를 보호하기 위해 다중 인증(MFA)이 구현됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.6.3	애플리케이션 및 시스템 계정과 관련 인증 요소의 사용은 엄격하게 관리됩니다. (PCI-DSS-v4.0)	access-keys-rotated	유효한 IAM 액세스 키가 maxAccessKeyAge에 지정된 일수에 따라 교체(변경)되는지 확인합니다. 지정된 기간 내에 액세스 키가 교체되지 않는 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
8.6.3	애플리케이션 및 시스템 계정과 관련 인증 요소의 사용은 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-check	AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. Secrets Manager는 교체가 이루어져야 하는 날짜를 계산합니다. 날짜가 경과하고 보안 암호가 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다.
8.6.3	애플리케이션 및 시스템 계정과 관련 인증 요소의 사용은 엄격하게 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	AWS Secrets Manager 보안 암호가 지난 지정된 일수 동안 교체되었는지 확인합니다. 보안 암호가 maxDaysSinceRotation 일수를 넘어 교체되지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 수동 DB 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. 기존 및 신규 Neptune 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
A1.1.2	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	api-gw-endpoint-type-check	Amazon API Gateway API가 규칙 파라미터 'endpointConfigurationType'에 지정된 유형인지 확인합니다. REST API가 규칙 파라미터에 구성된 엔드포인트 유형과 일치하지 않으면 규칙이 NON_COMPLIANT를 반환합니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Amazon CloudFront 배포가 웹 애플리케이션 방화벽(WAF) 또는 WAFv2 웹 액세스 제어 목록(ACL)과 연결되어 있는지 확인합니다. CloudFront 배포가 WAF 웹 ACL과 연결되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Amazon CloudFront 배포와 연결된 인증서가 기본 SSL 인증서가 아닌지 확인합니다. CloudFront 배포가 기본 SSL 인증서를 사용하는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-packets	AWS 네트워크 방화벽 정책이 조각화된 패킷에 대해 사용자 정의 상태 비저장 기본 작업으로 구성되어 있는지 확인합니다. 조각화된 패킷의 상태 비저장 기본 작업이 사용자 정의 기본 작업과 일치하지 않을 경우 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	rds-db-security-group-not-allowed	Amazon Relational Database Service(Amazon RDS) DB 보안 그룹이 기본 그룹인지 확인합니다. 기본 DB 보안 그룹이 아닌 DB 보안 그룹이 있는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	ec2-transit-gateway-auto-vpc-attach-disabled	Amazon Elastic Compute Cloud(Amazon EC2) Tranit Gateways에 'AutoAcceptSharedAttachments'가 활성화되어 있지 않았는지 확인합니다. 'AutoAcceptSharedAttachments'가 '활성화'로 설정된 경우 Transit Gateway의 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	eks-endpoint-no-public-access	Amazon Elastic Kubernetes Service(Amazon EKS) 엔드포인트에 대한 퍼블릭 액세스가 불가능한지 확인합니다. 엔드포인트가 퍼블릭 액세스 가능한 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	restricted-ssh	참고: 이 규칙의 경우 규칙 식별자(INCOMING_SSH_DISABLED)와 규칙 이름(restricted-ssh)이 서로 다릅니다. 보안 그룹의 SSH 수신 트래픽으로 액세스 가능한지 확인합니다. 보안 그룹의 SSH 수신 트래픽 IP 주소가 제한되면 규칙은 COMPLIANT입니다(0.0.0.0/0 또는 ::/0 이외의 CIDR). 그렇지 않으면 NON_COMPLIANT로 간주됩니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	appsync-associated-with-waf	AWS AppSync APIs AWS WAFv2 웹 액세스 제어 목록(ACLs)과 연결되어 있는지 확인합니다. 규칙은 웹 ACL과 연결되지 않은 경우 AWS AppSync API에 대한 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	codebuild-project-source-repo-url-check	Bitbucket 소스 리포지토리 URL에 로그인 보안 인증이 포함하고 있지 않는지 확인합니다. URL에 로그인 정보가 포함되어 있는 경우 규칙은 NON_COMPLIANT이고, 포함되지 않은 경우에는 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	elb-acm-certificate-required	Classic Load Balancer가 AWS Certificate Manager에서 제공하는 SSL 인증서를 사용하는지 확인합니다. 이 규칙을 적용하려면 Classic Load Balancer에서 SSL 또는 HTTPS 리스너를 사용합니다. 참고: 이 규칙은 Classic Load Balancer에만 적용됩니다. 이 규칙은 Application Load Balancer와 Network Load Balancer는 확인하지 않습니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	네트워크 액세스 제어 목록(NACL)에 대한 SSH/RDP 수신 트래픽의 기본 포트가 제한되는지 확인합니다. NACL 인바운드 엔트리가 포트 22 또는 3389에 대한 소스 TCP 또는 UDP CIDR 블록을 허용할 경우 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	waf-global-webacl-not-empty	WAF Global Web ACL에 일부 WAF 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않은 경우 이 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	waf-global-rulegroup-not-empty	AWS WAF Classic 규칙 그룹에 몇 가지 규칙이 포함되어 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	waf-global-rule-not-empty	AWS WAF 글로벌 규칙에 몇 가지 조건이 포함되어 있는지 확인합니다. WAF 글로벌 규칙 내에 조건이 없는 경우 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	ec2-client-vpn-not-authorize-all	AWS Client VPN 권한 부여 규칙이 모든 클라이언트에 대한 연결 액세스를 승인하지 않는지 확인합니다. 'AccessAll'이 존재하고 true로 설정된 경우 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인합니다. 인터넷 게이트웨이가 승인되지 않은 VPC에 연결된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A1.1.3	다중 테넌트 서비스 공급자는 모든 고객 환경과 데이터를 보호하고 분리합니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	api-gwv2-access-logs-enabled	Amazon API Gateway V2 단계에 액세스 로깅이 활성화되어 있는지 확인합니다. 단계 구성에 'accessLogSettings'가 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Amazon S3 버킷에 대한 액세스 로그를 전송하도록 Amazon CloudFront 배포가 구성되어 있는지 확인합니다. CloudFront 배포에 로깅이 구성되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	보안 모범 사례로 정의된 AWS CloudTrail 추적이 하나 이상 있는지 확인합니다. 다음을 모두 충족하는 추적이 하나 이상 있는 경우 이 규칙은 COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-export-enabled	Amazon Neptune 클러스터에 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있는지 확인합니다. Neptune 클러스터에서 감사 로그에 대해 CloudWatch 로그 내보내기가 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	ecs-task-definition-log-configuration	활성 ECS 태스크 정의에 logConfiguration이 설정되어 있는지 확인합니다. 활성 ECSTaskDefinition에 정의된 logConfiguration 리소스가 없거나, 하나 이상의 컨테이너 정의에서 logConfiguration 값이 null인 경우 이 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(CLOUD_TRAIL_ENABLED)와 규칙 이름(cloudtrail-enabled)이 다릅니다. AWS 계정에서 AWS CloudTrail 추적이 활성화되어 있는지 확인합니다. 추적이 활성화되지 않은 경우 규칙은 규정 미준수입니다. 선택적으로, 이 규칙은 특정 S3 버킷, Amazon Simple Notification Service(Amazon SNS) 주제 및 CloudWatch 로그 그룹을 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	참고: 이 규칙의 경우 규칙 식별자(MULTI_REGION_CLOUD_TRAIL_ENABLED)와 규칙 이름(multi-region-cloudtrail-enabled)이 서로 다릅니다. 다중 리전 AWS CloudTrail이 하나 이상 있는지 확인합니다. 추적이 입력 파라미터와 일치하지 않으면 규칙은 NON_COMPLIANT입니다. ExcludeManagementEventSources 필드가 비어 있지 않거나 AWS CloudTrail이 AWS KMS 이벤트 또는 Amazon RDS Data API 이벤트와 같은 관리 이벤트를 제외하도록 구성된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	appsync-logging-enabled	AWS AppSync API에 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 또는 'fieldLogLevel'이 ERROR 또는 ALL이 아닌 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	waf-classic-logging-enabled	AWS WAF 클래식 글로벌 웹 액세스 제어 목록(웹 ACLs)에서 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되어 있지 않은 경우 글로벌 웹 ACL에 대한 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-enabled	Amazon MQ 브로커에 Amazon CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-enabled	Amazon MQ 브로커에 CloudWatch 감사 로깅이 활성화되어 있는지 확인합니다. 브로커에 감사 로깅이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 로깅이 활성화된 상태로 구성되어 있는지 확인합니다. Amazon EKS 클러스터에 대한 로깅이 모든 로그 유형에 대해 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-cloudwatch	Amazon CloudWatch Logs로 로그를 전송하도록 AWS Elastic Beanstalk 환경이 구성되어 있는지 확인합니다. 'StreamLogs' 값이 false인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	step-functions-state-machine-logging-enabled	AWS Step Functions 시스템에 로깅이 활성화되어 있는지 확인합니다. 상태 시스템에 로깅이 활성화되어 있지 않거나, 로깅 구성이 제공된 최소 수준에 미치지 못할 경우 규칙은 NON_COMPLIANT입니다.
A1.2.1	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	netfw-logging-enabled	AWS Network Firewall 방화벽에 로깅이 활성화되어 있는지 확인합니다. 로깅 유형이 구성되지 않은 경우 이 규칙은 NON_COMPLIANT입니다. 규칙에서 확인할 로깅 유형을 지정할 수 있습니다.
A1.2.3	다중 테넌트 서비스 공급자는 모든 고객에 대한 로깅 및 인시던트 응답을 용이하게 합니다. (PCI-DSS-v4.0)	security-account-information-provided	AWS 계정 연락처에 대한 보안 연락처 정보를 제공했는지 확인합니다. 계정 내에 보안 연락처 정보가 제공되지 않은 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.2.5.1	PCI DSS 범위는 문서화되고 검증됩니다. (PCI-DSS-v4.0)	macie-auto-sensitive-data-discovery-check	Amazon Macie 에 민감한 데이터 자동 검색이 활성화되어 있는지 확인합니다. 민감한 데이터 자동 검색이 비활성화된 경우 규칙은 NON_COMPLIANT입니다. 이 규칙은 관리자 계정에는 APPLICABLE, 구성원 계정에는 NOT_APPLICABLE입니다.
A3.2.5.1	PCI DSS 범위는 문서화되고 검증됩니다. (PCI-DSS-v4.0)	macie-status-check	리전별 계정에서 Amazon Macie가 활성화되어 있는지 확인합니다. 'status' 속성이 'ENABLED'로 설정되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.2.5.2	PCI DSS 범위는 문서화되고 검증됩니다. (PCI-DSS-v4.0)	macie-auto-sensitive-data-discovery-check	Amazon Macie 에 민감한 데이터 자동 검색이 활성화되어 있는지 확인합니다. 민감한 데이터 자동 검색이 비활성화된 경우 규칙은 NON_COMPLIANT입니다. 이 규칙은 관리자 계정에는 APPLICABLE, 구성원 계정에는 NOT_APPLICABLE입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.2.5.2	PCI DSS 범위는 문서화되고 검증됩니다. (PCI-DSS-v4.0)	macie-status-check	리전별 계정에서 Amazon Macie가 활성화되어 있는지 확인합니다. 'status' 속성이 'ENABLED'로 설정되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation 스택이 Amazon SNS 주제로 이벤트 알림을 전송하는지 확인합니다. 필요한 경우 특정 Amazon SNS 주제가 사용되는지 여부를 확인합니다. CloudFormation 스택이 알림을 전송하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT 입니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	지정된 지표 이름의 CloudWatch 경보 설정이 지정한 설정과 일치하는지 확인합니다.
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig.CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.3.1	PCI DSS는 일상적 비즈니스(BAU) 활동에 통합됩니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-prohibited	Amazon Neptune 수동 DB 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. 기존 및 신규 Neptune 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-prohibited	Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭이 아닌지 확인합니다. Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	backup-recovery-point-manual-deletion-disabled	백업 볼트에 복구 지점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 백업 볼트에 리소스 기반 정책이 없거나, 적합한 'Deny' 문(backup:DeleteRecoveryPoint, backup:UpdateRecoveryPointLifecycle, backup:PutBackupVaultAccessPolicy permissions가 있는 문)이 없는 정책이 있는 경우 규칙은 NON_COMPLIANT입니다.
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	emr-block-public-access	Amazon EMR 계정에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. BlockPublicSecurityGroupRules가 false인 규칙은 NON_COMPLIANT입니다. 또는 true인 경우 포트 22 이외의 포트가 PermittedPublicSecurityGroupRuleRanges에 나열됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	secretsmanager-secret-unused	지정된 일수 내에 AWS Secrets Manager 보안 암호에 액세스했는지 확인합니다. 'unusedForDays' 일수 내에 보안 암호에 액세스하지 않은 경우 규칙은 NON_COMPLIANT입니다. 기본값은 90일입니다.
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	s3-access-point-public-access-blocks	Amazon S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있는지 확인합니다. S3 액세스 포인트에 대해 퍼블릭 액세스 차단 설정이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	s3-account-level-public-access-blocks	필요한 퍼블릭 액세스 차단 설정이 계정 수준에서 구성되어 있는지 확인합니다. 아래 설정된 필드가 구성 항목의 해당 필드와 일치하지 않는 경우에만 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.4.1	카드 소지자 데이터 환경에 대한 논리적 액세스는 제어 및 관리됩니다. (PCI-DSS-v4.0)	s3-bucket-mfa-delete-enabled	Amazon Simple Storage Service(Amazon S3) 버킷 버전 관리 구성에서 MFA Delete가 활성화되어 있는지 확인합니다. MFA Delete가 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	api-gw-xray-enabled	Amazon API Gateway REST APIs에서 AWS X-Ray 추적이 활성화되어 있는지 확인합니다. X-Ray 추적이 활성화된 경우 이 규정은 COMPLIANT이고, 그렇지 않은 경우 NON_COMPLIANT입니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	CloudFormation 스택이 Amazon SNS 주제로 이벤트 알림을 전송하는지 확인합니다. 필요한 경우 특정 Amazon SNS 주제가 사용되는지 여부를 확인합니다. CloudFormation 스택이 알림을 전송하지 않는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	ec2-instance-detailed-monitoring-enabled	EC2 인스턴스에 세부 모니터링이 활성화되어 있는지 확인합니다. 세부 모니터링이 활성화되지 않은 경우 규칙은 NON_COMPLIANT입니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	CloudWatch 경보에 ALARM, INSUFFICIENT_DATA 또는 OK 상태에 대해 구성된 작업이 있는지 확인합니다. 필요한 경우, 명명된 ARN과 일치하는 작업이 있는지 확인합니다. 경보 또는 선택적 파라미터에 대해 지정된 작업이 없는 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	리소스 유형에 지정된 지표에 대한 CloudWatch 경보가 있는지 확인합니다. 리소스 유형으로는 EBS 볼륨, EC2 인스턴스, Amazon RDS 클러스터 또는 S3 버킷을 지정할 수 있습니다. 지정된 지표에 리소스 ID와 CloudWatch 경보가 있는 경우 규칙은 규정을 COMPLIANT 입니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	지정된 지표 이름의 CloudWatch 경보 설정이 지정한 설정과 일치하는지 확인합니다.
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	wafv2-rulegroup-logging-enabled	AWS WAFv2 규칙 그룹에서 Amazon CloudWatch 보안 지표 수집이 활성화되어 있는지 확인합니다. 'VisibilityConfig. CloudWatchMetricsEnabled' 필드가 false로 설정된 경우 규칙은 NON_COMPLIANT입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
A3.5.1	의심스러운 이벤트를 식별하고 대응합니다. (PCI-DSS-v4.0)	sns-topic-message-delivery-notification-enabled	엔드포인트의 주제로 전송된 알림 메시지의 전송 상태에 대해 Amazon Simple Notification Service(SNS) 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되어 있지 않은 경우 규칙은 NON_COMPLIANT입니다.

템플릿

템플릿은 GitHub: PCI DSS 4.0(글로벌 리소스 유형 포함) 운영 모범 사례에서 확인할 수 있습니다.

공개적으로 액세스 가능한 리소스 운영 모범 사례

이 적합성 팩은 공개적으로 액세스할 수 있는 리소스를 식별하는 데 도움이 됩니다.

에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 공개적으로 액세스할 수 있는 리소스 운영 모범 사례에서 확인할 수 있습니다.

UCB용 RBI 사이버 보안 프레임워크 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Reserve Bank of India(RBI) Urban Cooperative Banks(UCBs)용 사이버 보안 프레임워크와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되

며 UCBs. UCB 제어를 위한 RBI 사이버 보안 프레임워크는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.1)	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
Annex_I(1.1)	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.
Annex_I(1.1)	ecr-private-tag-immutability-enabled	Elastic Container Repository(ECR) 태그 변경 불가능 기능을 활성화하여 ECR 이미지의 이미지 태그를 덮어쓰지 않도록 합니다. 이전에는 태그를 덮어쓸 수 있었기 때문에 이미지를 고유하게 식별하기 위한 수동 방법이 필요했습니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
Annex_I(1.3)	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	api-gw-cache-enabled-and-encrypted	저장 데이터를 보호하려면 API Gateway 단계의 캐시에 암호화가 활성화되어 있어야 합니다. API 메서드에서 민감한 데이터를 캡처할 수 있으므로 저장 중 암호화를 활성화하면 해당 데이터를 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.
Annex_I(1.3)	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
Annex_I(1.3)	elb-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Annex_I(1.3)	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.
Annex_I(1.3)	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.
Annex_I(1.3)	backup-recovery-point-encrypted	AWS 백업 복구 시점에 암호화가 활성화되어 있는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	codebuild-project-artifact-encryption	저장 시 민감한 데이터를 보호하려면 AWS CodeBuild 아티팩트에 암호화가 활성화되어 있는지 확인하세요.
Annex_I(1.3)	codebuild-project-s3-logs-encrypted	저장 시 민감한 데이터를 보호하려면 Amazon S3에 저장된 AWS CodeBuild 로그에 대해 암호화가 활성화되어 있는지 확인합니다.
Annex_I(1.3)	opensearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
Annex_I(1.3)	opensearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	dynamodb-table-encrypted-kms	Amazon DynamoDB 테이블에 대해 암호화가 활성화되었는지 확인합니다. 이러한 테이블에 민감한 데이터가 저장 중일 수 있으므로 저장 암호화를 활성화하여 해당 데이터를 보호합니다. 기본적으로 DynamoDB 테이블은 AWS 소유 고객 마스터 키(CMK)로 암호화됩니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
Annex_I(1.3)	elasticsearch-encrypted-at-rest	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service(OpenSearch Service) 도메인에서 암호화가 활성화되어 있는지 확인합니다.
Annex_I(1.3)	elasticsearch-node-to-node-encryption-check	Amazon OpenSearch Service를 위한 노드 간 암호화가 활성화되어 있는지 확인합니다. 노드 간 암호화를 사용하면 Amazon Virtual Private Cloud(VPC) 내 모든 통신에 대해 TLS 1.2 암호화를 사용할 수 있습니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
Annex_I(1.3)	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.
Annex_I(1.3)	rds-snapshot-encrypted	Amazon Relational Database Service(RDS) 스냅샷에 대해 암호화가 활성화되었는지 확인합니다. 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	rds-storage-encrypted	저장 데이터를 보호하기 위해 Amazon Relational Database Service(RDS) 인스턴스에 대해 암호화가 활성화되었는지 확인합니다. Amazon RDS 인스턴스에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.
Annex_I(1.3)	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	sagemaker-endpoint-configuration-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 엔드포인트에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 엔드포인트에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	sagemaker-notebook-instance-kms-key-configured	저장 데이터를 보호하기 위해 SageMaker 노트북에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. SageMaker 노트북에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Annex_I(1.3)	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Annex_I(1.3)	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
Annex_I(1.3)	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.
Annex_I(1.3)	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	no-unrestricted-route-to-igw	Amazon EC2 라우팅 테이블에는 인터넷 게이트웨이에 대한 무제한 경로가 없어야 합니다. Amazon VPC 내 워크로드의 인터넷 액세스를 제거하거나 제한하면 환경 내에서 의도하지 않은 액세스를 줄일 수 있습니다.
Annex_I(1.3)	redshift-cluster-kms-enabled	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 AWS Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Redshift 클러스터에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
Annex_I(1.3)	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.
Annex_I(1.3)	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
Annex_I(1.3)	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
Annex_I(1.3)	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
Annex_I(1.3)	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.
Annex_I(1.3)	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
Annex_I(1.3)	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(1.3)	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
Annex_I(1.3)	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
Annex_I(5.1)	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(5.1)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
Annex_I(5.1)	waf-regional-rule-not-empty	AWS WAF에 비어 있지 않은 규칙이 있는지 확인합니다. 조건이 없는 규칙에는 의도하지 않은 동작이 발생할 수 있습니다.
Annex_I(5.1)	waf-regional-rulegroup-not-empty	AWS WAF에 비어 있지 않은 규칙 그룹이 있는지 확인합니다. 규칙 그룹이 비어 있으면 의도하지 않은 동작이 발생할 수 있습니다.
Annex_I(5.1)	waf-regional-webacl-not-empty	AWS WAF에 연결된 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우 WAF에서 탐지하거나 조치를 취하지 않고 웹 트래픽이 전달됩니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(5.1)	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.
Annex_I(5.1)	api-gw-associated-with-waf	AWS WAF를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트(웹 액세스 제어 목록(웹 ACL)이라고 함)를 구성할 수 있습니다. 악의적인 공격으로부터 보호하기 위해 Amazon API Gateway 스테이지가 WAF 웹 ACL과 연결되어 있도록 합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(5.1)	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
Annex_I(5.1)	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(6)	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경 세부 정보의 기준을 설정할 수 있습니다.
Annex_I(6)	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(6)	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
Annex_I(6)	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.
Annex_I(6)	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(6)	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
Annex_I(6)	vuln-management-plan-exists (프로세스 확인)	사용자 환경의 취약성을 해결하기 위한 프로세스를 공식적으로 정의하려면 취약성 관리 계획을 개발하고 구현해야 합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(7.1)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 되며, 정책이 "Effect": "Allow" with "Action": "*" over "Resource": "*"를 포함하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Annex_I(7.1)	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
Annex_I(7.1)	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(7.1)	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
Annex_I(7.1)	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(7.2)	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(7.3)	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
Annex_I(7.4)	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
Annex_I(7.4)	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
Annex_I(7.4)	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
Annex_I(7.4)	cloudtrail-s3-dataevents-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.
Annex_I(7.4)	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(7.4)	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
Annex_I(7.4)	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
Annex_I(7.4)	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(7.4)	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.
Annex_I(7.4)	opensearch-audit-logging-enabled	Amazon OpenSearch Service 도메인에서 감사 로깅이 활성화되었는지 확인합니다. 감사 로깅을 사용하면 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경, 들어오는 검색 쿼리를 포함하여 OpenSearch 도메인에서의 사용자 활동을 추적할 수 있습니다.
Annex_I(7.4)	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
Annex_I(7.4)	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(7.4)	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.
Annex_I(7.4)	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(7.4)	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.
Annex_I(7.4)	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(7.4)	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.
Annex_I(7.4)	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted (Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(10.2)	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.
Annex_I(12)	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
Annex_I(12)	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(12)	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.
Annex_I(12)	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Annex_I(12)	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(12)	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Annex_I(12)	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(12)	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
Annex_I(12)	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	AWS 구성 규칙	지침
Annex_I(12)	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
Annex_I(12)	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
Annex_I(12)	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

템플릿

템플릿은 GitHub: UCB용 RBI 사이버 보안 프레임워크 운영 모범 사례에서 확인할 수 있습니다.

RBI MD-ITF 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 Reserve Bank of India(RBI) 마스터 방향 - 정보 기술 프레임워크와 AWS 관리형 Config 규칙 간의 샘플 매핑을 제공합니다. 각 Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 RBI 마스터 방향 - 정보 기술 프레임워크 제어와 관련이 있습니다. RBI 정보 기술 프레임워크 마스터 지침 내 제어는 여러 Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(a)	정보 자산의 식별 및 분류	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한

제어 ID	제어 설명	AWS 구성 규칙	지침
			기타 세부 정보를 제공합니다.
3.1(a)	정보 자산의 식별 및 분류	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
3.1(a)	정보 자산의 식별 및 분류	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능이라는 개념을 위반할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(a)	정보 자산의 식별 및 분류	ecr-private-tag-immutability-enabled	Elastic Container Repository(ECR) 태그 변경 불가능 기능을 활성화하여 ECR 이미지의 이미지 태그를 덮어쓰지 않도록 합니다. 이전에는 태그를 덮어쓸 수 있었기 때문에 이미지를 고유하게 식별하기 위한 수동 방법이 필요했습니다.
3.1(c)	역할 기반 액세스 제어	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(c)	역할 기반 액세스 제어	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(c)	역할 기반 액세스 제어	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.
3.1(c)	역할 기반 액세스 제어	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(c)	역할 기반 액세스 제어	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.
3.1(c)	역할 기반 액세스 제어	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(c)	역할 기반 액세스 제어	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(c)	역할 기반 액세스 제어	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
3.1(c)	역할 기반 액세스 제어	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
3.1(c)	역할 기반 액세스 제어	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(c)	역할 기반 액세스 제어	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
3.1(c)	역할 기반 액세스 제어	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(c)	역할 기반 액세스 제어	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
3.1(c)	역할 기반 액세스 제어	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(c)	역할 기반 액세스 제어	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
3.1(c)	역할 기반 액세스 제어	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(c)	역할 기반 액세스 제어	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(c)	역할 기반 액세스 제어	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
3.1(c)	역할 기반 액세스 제어	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(c)	역할 기반 액세스 제어	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
3.1(c)	역할 기반 액세스 제어	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(g)	인시던트 관리	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
3.1(g)	인시던트 관리	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(g)	인시던트 관리	alb-waf-enabled	웹 애플리케이션을 보호하기 위해 Elastic Load Balancer(ELB)에서 AWS WAF가 활성화되어 있는지 확인합니다. WAF는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 됩니다. 이러한 웹 익스플로잇은 사용자 환경에서 가용성에 영향을 미치거나 보안을 손상시킬 수 있으며 혹은 리소스를 과도하게 사용할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(g)	인시던트 관리	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.
3.1(g)	인시던트 관리	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(h)	추적	api-gw-execution-logging-enabled	API Gateway 로깅에는 API에 액세스한 사용자 및 액세스 방식에 관한 세부 정보 보기가 표시됩니다. 이러한 인사이트를 통해 사용자 활동을 파악할 수 있습니다.
3.1(h)	추적	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
3.1(h)	추적	codebuild-project-logging-enabled	빌드 출력 로그가 Amazon CloudWatch 또는 Amazon Simple Storage Service(Amazon S3)로 전송되도록 Ensure AWS CodeBuild 프로젝트 로깅이 활성화되어 있습니다. 빌드 출력 로그는 빌드 프로젝트에 관한 자세한 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(h)	추적	opensearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. OpenSearch Service 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.
3.1(h)	추적	redshift-audit-logging-enabled	Amazon Redshift 클러스터의 연결 및 사용자 활동에 대한 정보를 캡처하려면 감사 로깅이 활성화되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(h)	추적	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
3.1(h)	추적	cloudtrail-s3-data events-enabled	Amazon Simple Storage Service(S3) 데이터 이벤트를 수집하면 모든 변칙적 활동을 탐지하는 데 도움이 됩니다. 세부 정보에는 Amazon S3 버킷에 액세스한 AWS 계정 정보, IP 주소 및 이벤트 시간이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(h)	추적	cw-loggroup-retention-period-check	문제 해결 및 포렌식 조사에 도움이 되도록 로그 그룹에 대한 이벤트 로그 데이터를 최소 기간 동안 유지하세요. 사용 가능한 과거 이벤트 로그 데이터가 부족하면 잠재적으로 악의적인 이벤트를 재구성하고 식별하기가 어렵습니다.
3.1(h)	추적	elasticsearch-logs-to-cloudwatch	Amazon OpenSearch Service 도메인에 오류 로그가 활성화되어 있고 보존 및 대응을 위해 Amazon CloudWatch Logs로 스트리밍되는지 확인하세요. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(h)	추적	elb-logging-enabled	Elastic Load Balancing 활동은 환경 내 통신의 중심 지점입니다. ELB 로깅이 활성화되었는지 확인합니다. 수집된 데이터는 ELB로 전송된 요청에 관한 자세한 정보를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(h)	추적	multi-region-cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록합니다. 호출된 사용자 및 계정 AWS, 호출이 수행된 원본 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. MULTI_REGION_CLOUD_TRAIL_ENABLED 가 활성화된 경우 CloudTrail은 모든 AWS 리전의 로그 파일을 S3 버킷으로 전송합니다. 또한가 새 리전을 AWS 시작하면 CloudTrail은 새 리전에서 동일한 추적을 생성합니다. 따라서 별도의 조치를 취하지 않아도 새 리전의 API 활동이 포함된 로그 파일을 받게 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(h)	추적	rds-logging-enabled	환경 내에서 로깅 및 모니터링에 도움이 되도록 Amazon Relational Database Service(RDS) 로깅이 활성화되어 있는지 확인합니다. Amazon RDS 로깅을 사용하면 연결, 연결 끊김, 쿼리 또는 쿼리된 테이블과 같은 이벤트를 캡처할 수 있습니다.
3.1(h)	추적	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(h)	추적	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.
3.1(h)	추적	wafv2-logging-enabled	환경 내에서 로깅 및 모니터링을 지원하려면 리전 및 글로벌 웹 ACLs에서 AWS WAF(V2) 로깅을 활성화합니다. AWS WAF 로깅은 웹 ACL에서 분석하는 트래픽에 대한 자세한 정보를 제공합니다. 로그에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 정보 및 각 요청이 일치하는 규칙에 대한 작업이 기록됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(h)	추적	redshift-cluster-configuration-check	저장 데이터를 보호하기 위해 Amazon Redshift 클러스터에 대해 암호화가 활성화되어 있는지 확인합니다. 또한 필수 구성이 Amazon Redshift 클러스터에 배포되었는지 확인해야 합니다. 데이터베이스의 연결 및 사용자 활동에 관한 정보를 제공하려면 감사 로깅을 활성화해야 합니다. 이 규칙을 사용하려면 clusterDbEncrypted(Config 기본값: TRUE) 및 loggingEnabled(Config 기본값: TRUE)에 대한 값을 설정해야 합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(i)	퍼블릭 키 인프라	acm-certificate-expiration-check	AWS ACM에서 X509 인증서를 발급하여 네트워크 무결성을 보호합니다. 이러한 인증서는 유효하고 만료되지 않은 것이어야 합니다. 이 규칙에는 daysToExpiration(AWS 기본 보안 모범 사례 값: 90) 값이 필요합니다. 실제 값은 조직의 정책을 반영해야 합니다.
3.1(i)	퍼블릭 키 인프라	alb-http-drop-invalid-header-enabled	Elastic Load Balancer(ELB)가 http 헤더를 삭제하도록 구성되었는지 확인합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1(i)	퍼블릭 키 인프라	alb-http-to-https-redirection-check	전송 중 데이터를 보호하려면 Application Load Balancer가 암호화되지 않은 HTTP 요청을 자동으로 HTTPS로 리디렉션하도록 해야 합니다. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(i)	퍼블릭 키 인프라	api-gw-ssl-enabled	Amazon API Gateway REST API 스테이지를 SSL 인증서로 구성하여 요청이 API Gateway에서 시작되었음을 백엔드 시스템이 인증할 수 있도록 합니다.
3.1(i)	퍼블릭 키 인프라	opensearch-https-required	민감한 데이터가 존재할 수 있으므로 전송 중 데이터를 보호하는 데 도움이 되도록 Amazon OpenSearch Service 도메인에서 HTTPS가 활성화되어 있는지 확인합니다.
3.1(i)	퍼블릭 키 인프라	elbv2-acm-certificate-required	민감한 데이터가 존재할 수 있고 전송 시 데이터를 보호하는 데 도움이 되므로 Elastic Load Balancing에서 암호화를 활성화해야 합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(i)	퍼블릭 키 인프라	elb-acm-certificate-required	민감한 데이터가 존재할 수 있으므로 전송 시 데이터를 보호하는 데 도움이 되도록 Elastic Load Balancing에 대해 암호화가 활성화되었는지 확인합니다. AWS Certificate Manager를 사용하여 AWS 서비스 및 내부 리소스를 사용하여 퍼블릭 및 프라이빗 SSL/TLS 인증서를 관리, 프로비저닝 및 배포합니다.
3.1(i)	퍼블릭 키 인프라	elb-tls-https-listeners-only	Elastic Load Balancer(ELB)가 SSL 또는 HTTPS 리스너로 구성되어 있는지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.1(i)	퍼블릭 키 인프라	redshift-require-tls-ssl	Amazon Redshift 클러스터를 SQL 클라이언트에 연결하려면 TLS/SSL 암호화가 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.1(i)	퍼블릭 키 인프라	s3-bucket-ssl-requests-only	전송 중 데이터 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 보안 소켓 계층(SSL) 사용 요청이 필요한지 확인하세요. 민감한 데이터가 존재할 수 있으므로 전송 중 암호화를 활성화하여 해당 데이터를 보호합니다.
3.3	취약성 관리	elastic-beanstalk-managed-updates-enabled	Amazon Elastic Beanstalk 환경에서 관리형 플랫폼 업데이트를 활성화하면 사용 가능한 최신 플랫폼 수정, 업데이트 및 환경 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것이 시스템 보안의 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	취약성 관리	rds-automatic-minor-version-upgrade-enabled	Amazon RDS(Relational Database Service) 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하여 관계형 데이터베이스 관리 시스템(RDBMS)의 최신 마이너 버전 업데이트가 설치되도록 합니다. 여기에는 보안 패치 및 버그 수정이 포함될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	취약성 관리	redshift-cluster-maintenancesettings-check	이 규칙은 Amazon Redshift 클러스터가 조직에서 선호하는 설정을 갖도록 보장합니다. 특히 데이터베이스에 기본 설정된 유지 관리 기간과 자동화된 스냅샷 보존 기간이 있습니다. 이 규칙을 사용하려면 allowVersionUpgrade를 설정해야 합니다. 기본값은 true입니다. 선택적으로 preferredMaintenanceWindow(기본값은 sat:16:00-sat:16:30)와 automatedSnapshotRetentionPeriod(기본값은 1)도 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	취약성 관리	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	취약성 관리	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.3	취약성 관리	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
3.3	취약성 관리	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5	사이버 위기 관리 계획	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.
3.5	사이버 위기 관리 계획	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5	사이버 위기 관리 계획	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.5	사이버 위기 관리 계획	ec2-managedinstance-association-compliance-status-check	AWS Systems Manager Associations를 사용하여 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 지원합니다. AWS Systems Manager는 관리형 인스턴스에 구성 상태를 할당하고 운영 체제 패치 수준, 소프트웨어 설치, 애플리케이션 구성 및 기타 환경에 대한 세부 정보의 기준을 설정할 수 있습니다.
3.5	사이버 위기 관리 계획	ec2-managedinstance-patch-compliance-status-check	이 규칙을 활성화하면 Amazon Elastic Compute Cloud(Amazon EC2) 취약성을 식별하고 문서화하는 데 도움이 됩니다. 규칙은 조직의 정책 및 절차에 따라 AWS Systems Manager에서 Amazon EC2 인스턴스 패치 규정 준수 여부를 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
3.9	IT 위험 평가	annual-risk-assessment-performed(프로세스 확인)	조직에 대한 연간 위험 평가를 수행합니다. 위험 평가는 식별된 위험 및/또는 취약성이 조직에 영향을 미칠 가능성과 영향을 파악하는 데 도움이 될 수 있습니다.
3.12	학습	security-awareness-program-exists(프로세스 확인)	조직을 위한 보안 인식 프로그램을 수립하고 유지합니다. 보안 인식 프로그램은 다양한 보안 침해나 사고로부터 조직을 보호하는 방법을 직원들에게 교육합니다.
4.4(g)	사기 분석- 의심스러운 거래 분석, 횡령, 절도 또는 의심되는 자금 세탁, 자산 남용, 재무 기록 조작 등 RBI에 사기를 신고하기 위한 규제 요건은 시스템에 기반해야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	clb-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	elbv2-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	lambda-vpc-multi-az-check	AWS Lambda 함수가 계정의 Virtual Private Cloud(VPC)에 연결되도록 구성된 경우, 최소 두 개의 서로 다른 가용 영역에 AWS Lambda 함수를 배포하여 단일 영역에서 서비스 중단이 발생할 경우 이벤트를 처리할 수 있는 함수인지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	s3-bucket-default-lock-enabled	Amazon Simple Storage Service(S3) 버킷에 기본적으로 잠금이 활성화되어 있는지 확인합니다. S3 버킷에 저장 중 민감한 데이터가 있을 수 있으므로 해당 데이터를 보호할 수 있도록 저장 시 객체 잠금을 적용합니다.
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	lambda-dlq-check	이 규칙을 활성화하면 함수가 실패했을 때 Amazon Simple Queue Service(Amazon SQS) 또는 Amazon Simple Notification Service(SNS)를 통해 담당 직원에게 알리는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 향상된 상태 보고를 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다. Elastic Beanstalk 강화된 상태 보고는 식별된 문제의 심각도를 판단하고 조사할 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	ebs-optimized-instance	Amazon Elastic Block Store(Amazon EBS)의 최적화된 인스턴스는 Amazon EBS I/O 작업을 위한 추가 전용 용량을 제공합니다. 이 최적화는 Amazon EBS I/O 작업과 인스턴스의 기타 트래픽 간의 경합을 최소화하여 EBS 볼륨에 가장 효율적인 성능을 제공합니다.
4.4(h)	IT 보안 시스템의 용량 및 성능 분석	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
4.4(i)	사고 보고, 이에 따른 영향 및 향후 이러한 사건이 재발하지 않도록 취한 조치	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
4.4(i)	사고 보고, 이에 따른 영향 및 향후 이러한 사건이 재발하지 않도록 취한 조치	guardduty-non-archived-findings	Amazon GuardDuty는 조사 결과를 심각도(낮음, 중간, 높음)로 분류하여 인시던트의 영향을 이해하는 데 도움이 됩니다. 이러한 분류를 사용하여 해결 전략 및 우선 순위를 결정할 수 있습니다. 이 규칙을 사용하면 조직의 정책에 따라 보관되지 않은 검색 결과에 대해 daysLowSev(Config 기본값: 30), daysMediumSev(Config 기본값: 7) 및 daysHighSev(Config 기본값: 1)를 선택적으로 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	aurora-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Aurora 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	cmk-backing-key-rotation-enabled	키 교체를 활성화하여 암호화 기간 종료 후 키를 교체하도록 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	ec2-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Compute Cloud(Amazon EC2) 리소스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	fsx-resources-protected-by-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon FSx 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.
6.3	NBFC는 중요한 비즈니스 시스템 및 데이터 센터에 필요한 백업 사이트를 마련할 필요성을 고려해야 합니다.	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling은 AWS Application Auto Scaling 서비스를 사용하여 실제 트래픽 패턴에 자동으로 응답하는 프로비저닝된 처리량 용량을 조정합니다. 따라서 테이블 또는 글로벌 보조 인덱스에 따라 할당된 읽기/쓰기 용량을 늘려 제한 없이 갑작스러운 트래픽 증가를 처리할 수 있습니다.
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	elb-cross-zone-load-balancing-enabled	Elastic Load Balancer(ELB)의 영역 간 로드 밸런싱 활성화는 적절한 용량과 가용성을 유지하는 데 도움이 됩니다. 영역 간 로드 밸런싱을 사용하면 활성화된 각 가용성 영역에서 동일한 수의 인스턴스를 유지해야 할 필요성이 줄어듭니다. 또한 애플리케이션이 보다 효과적으로 하나 이상의 인스턴스 손실을 처리할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	elb-deletion-protection-enabled	이 규칙은 Elastic Load Balancing이 삭제 방지 기능을 사용하도록 합니다. 이 기능을 사용하면 로드 밸런서가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	clb-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	elbv2-multiple-az	Elastic Load Balancing(ELB)은 하나의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. 고가용성을 보장하려면 ELB에 여러 가용 영역의 인스턴스가 등록되어 있어야 합니다.
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	lambda-vpc-multi-az-check	AWS Lambda 함수가 계정의 Virtual Private Cloud(VPC)에 연결되도록 구성된 경우, 최소 두 개의 서로 다른 가용 영역에 AWS Lambda 함수를 배포하여 단일 영역에서 서비스 중단이 발생할 경우 이벤트를 처리할 수 있는 함수인지 확인합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	rds-instance-deletion-protection-enabled	Amazon Relational Database Service(RDS) 인스턴스에 삭제 방지 기능이 활성화되어 있는지 확인하세요. 삭제 방지를 사용하면 Amazon RDS 인스턴스가 실수로 또는 악의적으로 삭제되어 애플리케이션의 가용성이 손실되는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	rds-multi-az-support	Amazon Relational Database Service(RDS)의 다중 AZ 지원은 데이터베이스 인스턴스의 가용성과 내구성을 향상시킵니다. 다중 AZ 데이터베이스 인스턴스를 프로비저닝하면 Amazon RDS가 자동으로 기본 데이터베이스 인스턴스를 생성하고 다른 가용 영역에 있는 대기 인스턴스에 데이터를 동기식으로 복제합니다. 각 가용 영역은 물리적으로 구분된 자체 독립 인프라에서 실행되며 안정성이 높도록 설계되었습니다. 인프라 장애가 발생할 경우, Amazon RDS는 대기 인프라로 자동 장애 조치를 수행하므로 장애 조치가 완료되는 즉시 데이터베이스 작업을 재개할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	vpc-vpn-2-tunnels-up	중복되는 Site-to-Site VPN 터널을 구현하여 복원력 요구 사항을 달성할 수 있습니다. 두 개의 터널을 사용하여 Site-to-Site VPN 연결 중 하나를 사용할 수 없는 경우를 대비하고 계속적인 연결을 보장합니다. 고객 게이트웨이를 사용할 수 없을 때 연결이 끊어지지 않도록, 두 번째 고객 게이트웨이를 사용하여 Amazon Virtual Private Cloud(VPC)와 가상 프라이빗 게이트웨이에 대한 두 번째 Site-to-Site VPN 연결을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud(Amazon EC2) Auto Scaling 그룹의 Elastic Load Balancer(ELB) 상태 확인은 적절한 용량과 가용성의 유지 관리를 지원합니다. 로드 밸런서가 정기적으로 ping을 전송하거나, 연결을 시도하거나, 요청을 전송하여 Auto Scaling 그룹의 Amazon EC2 인스턴스 상태를 테스트합니다. 인스턴스가 다시 보고하지 않는 경우 트래픽은 새 Amazon EC2 인스턴스로 전송됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	dynamodb-throughput-limit-check	Amazon DynamoDB 테이블에서 프로비저닝된 처리 용량을 확인하려면 이 규칙을 활성화하세요. 이는 각 테이블에서 지원할 수 있는 읽기 및 쓰기 활동의 양입니다. DynamoDB는 이 정보를 사용하여 처리량 요구 사항에 맞는 충분한 시스템 리소스를 예약합니다. 이 규칙은 처리량이 고객 계정의 최대 한도에 도달하면 알림을 생성합니다. 이 규칙을 사용하면 선택적으로 accountRCUThresholdPercentage(Config 기본값: 80) 및 accountWCUThresholdPercentage(Config 기본값: 80) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	lambda-concurrency-check	이 규칙은 Lambda 함수의 동시성 상한 및 하한이 설정되도록 합니다. 이는 특정 시점에 함수가 처리하는 요청 수에 대한 기준 설정에 도움이 될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	rds-enhanced-monitoring-enabled	Amazon Relational Database Service(RDS)를 활성화함으로써 Amazon RDS 가용성을 모니터링하는 데 도움이 됩니다. 이를 통해 Amazon RDS 데이터베이스 인스턴스의 상태를 자세히 파악할 수 있습니다. Amazon RDS 스토리지가 두 개 이상의 기본 물리적 디바이스를 사용하는 경우, 향상된 모니터링은 각 디바이스에 대한 데이터를 수집합니다. 또한 Amazon RDS 데이터베이스 인스턴스가 다중 AZ 배포에서 실행되는 경우, 보조 호스트의 각 디바이스에 대한 데이터와 보조 호스트 지표가 수집됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.1	NBFC 운영의 규모와 복잡성이 증가함에 따라 IT 시스템을 점진적으로 확장해야 합니다.	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Management) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	dms-replication-not-public	DMS 복제 인스턴스에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. DMS 복제 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	ebs-snapshot-public-restorable-check	EBS 스냅샷을 공개적으로 복원할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. EBS 볼륨 스냅샷에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	elasticsearch-in-vpc-only	Amazon OpenSearch Service(OpenSearch Service) 도메인이 Amazon Virtual Private Cloud(Amazon VPC) 내에 있는지 AWS 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 OpenSearch Service와 다른 서비스 간에 보안 통신이 가능합니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	emr-master-no-public-ip	Amazon EMR 클러스터 마스터 노드에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드에 대한 액세스를 관리합니다. Amazon EMR 클러스터 프라이머리 노드에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	rds-instance-public-access-check	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	rds-snapshots-public-prohibited	Amazon Relational Database Service(Amazon RDS) 인스턴스가 공개되지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon RDS 데이터베이스 인스턴스에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	redshift-cluster-public-access-check	Amazon Redshift 클러스터가 퍼블릭이 아닌지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Redshift 클러스터에는 민감한 정보와 원칙이 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	sagemaker-notebook-no-direct-internet-access	Amazon SageMaker 노트북에서 직접 인터넷 액세스를 허용하지 않도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 직접 인터넷 액세스를 방지함으로써 권한이 없는 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	emr-kerberos-enabled	Amazon EMR 클러스터용 Kerberos를 활성화하면 액세스 권한 및 권한 부여를 관리하고 최소 권한 및 업무 분리 원칙에 따라 통합할 수 있습니다. Kerberos에서는 인증이 필요한 서비스 및 사용자를 보안 주체라고 합니다. 보안 주체는 Kerberos 영역 내에 존재합니다. 영역 내에서 Kerberos 서버는 키 배포 센터(KDC)로 알려져 있습니다. 이는 보안 주체가 인증할 수 있는 수단을 제공합니다. KDC는 인증을 위한 티켓을 발급하여 인증합니다. KDC는 영역 내의 보안 주체, 그들의 암호 및 각 보안 주체에 대한 기타 관리자 정보가 저장된 데이터베이스를 유지합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	iam-group-has-users-check	AWS Identity and Access Managemen t(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	autoscaling-launch-config-public-ip-disabled	퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스에 연결된 리소스에 도달할 수 있습니다. EC2 리소스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 애플리케이션이나 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	ecs-task-definition-nonroot-user	최소 권한 원칙을 구현하는 데 도움이 되도록 루트 사용자가 아닌 사용자가 Amazon Elastic Container Service(Amazon ECS) 작업 정의에 대해 액세스 권한이 있는지 확인합니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	efs-access-point-enforce-root-directory	Amazon Elastic File System(Amazon EFS) 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	efs-access-point-enforce-user-identity	최소 권한 원칙을 구현하는 데 도움이 되도록 Amazon Elastic File System(Amazon EFS)에 대해 사용자 적용이 활성화되어 있어야 합니다. 활성화되면 Amazon EFS는 NFS 클라이언트의 사용자 및 그룹 ID를 모든 파일 시스템 작업의 액세스 포인트에 구성된 ID로 대체하고, 적용된 이 사용자 ID에 대한 액세스 권한만 부여합니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Management(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	subnet-auto-assign-public-ip-disabled	Amazon Virtual Private AWS Cloud(VPC) 서브넷에 퍼블릭 IP 주소가 자동으로 할당되지 않도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 이 속성이 활성화된 서브넷에서 시작되는 Amazon Elastic Compute Cloud(EC2) 인스턴스에는 기본 네트워크 인터페이스에 할당된 퍼블릭 IP 주소가 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Management(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합하는 데 도움이 됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Managemen t(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	opensearch-in-vpc-only	Amazon OpenSearch Service 도메인이 Amazon Virtual Private AWS Cloud(Amazon VPC) 내에 있는지 확인하여 클라우드에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud Amazon OpenSearch Service 도메인이 Amazon VPC 안에 있으면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 Amazon OpenSearch Service 와 다른 서비스 간에 보안 통신이 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.I	물리적/논리적 액세스 제어 및 잘 정의된 암호 정책과 같은 기본 보안 측면	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
8.II	잘 정의된 사용자 역할	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.II	잘 정의된 사용자 역할	iam-no-inline-policy-check	AWS Identity and Access Managemen t(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다.는 인라인 정책 대신 관리형 정책을 사용하도록 AWS 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.II	잘 정의된 사용자 역할	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은

제어 ID	제어 설명	AWS 구성 규칙	지침
			조직의 정책을 반영해야 합니다.
8.II	잘 정의된 사용자 역할	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management(IAM)는 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하는 데 도움이 될 수 있으며, 정책이 "Effect": "Allow"를 "Action": "*"를 사용하여 "Resource": "*"를 포함하도록 제한합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.
8.II	잘 정의된 사용자 역할	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.II	잘 정의된 사용자 역할	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
8.II	잘 정의된 사용자 역할	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.III	오류 및 오용의 위험을 줄이고 데이터 및 정보의 신뢰성을 보장하기 위한 생성자-확인자 개념	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
8.IX	주기적 테스트를 통한 데이터 백업 준비	db-instance-backup-enabled	Amazon RDS의 백업 기능은 데이터베이스 및 트랜잭션 로그의 백업을 생성합니다. Amazon RDS는 전체 DB 인스턴스를 백업하여 DB 인스턴스의 스토리지 볼륨 스냅샷을 생성합니다. 시스템에서 복원력 요구 사항을 충족하도록 특정 보존 기간을 설정할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.IX	주기적 테스트를 통한 데이터 백업 준비	dynamodb-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon DynamoDB 테이블이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
8.IX	주기적 테스트를 통한 데이터 백업 준비	dynamodb-pitr-enabled	이 규칙을 사용하면 정보가 백업되었는지 확인할 수 있습니다. 또한 Amazon DynamoDB에서 특정 시점으로 복구를 활성화하여 백업을 유지합니다. 복구를 통해 지난 35일 동안의 테이블 연속 백업이 유지됩니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.IX	주기적 테스트를 통한 데이터 백업 준비	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
8.IX	주기적 테스트를 통한 데이터 백업 준비	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.IX	주기적 테스트를 통한 데이터 백업 준비	elasticache-redis-cluster-automatic-backup-check	자동 백업이 활성화되면 Amazon ElastiCache에서 매일 클러스터 백업을 생성합니다. 백업은 조직에서 지정한 기간 동안 유지할 수 있습니다. 자동 백업은 데이터 손실을 막는 데 도움이 됩니다. 장애가 발생할 경우 새로운 클러스터를 생성해 최신 백업에서 모든 데이터를 복원할 수 있습니다.
8.IX	주기적 테스트를 통한 데이터 백업 준비	rds-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Relational Database Service(Amazon RDS) 인스턴스가 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.IX	주기적 테스트를 통한 데이터 백업 준비	s3-bucket-replication-enabled	Amazon Simple Storage Service(S3) 교차 리전 복제(CRR)는 적절한 용량과 가용성을 유지할 수 있도록 지원합니다. CRR은 Amazon S3 버킷 전체에 걸쳐 객체를 비동기식으로 자동 복사할 수 있으므로 데이터 가용성 유지에 도움이 됩니다.
8.IX	주기적 테스트를 통한 데이터 백업 준비	redshift-backup-enabled	데이터 백업 프로세스에 도움이 되도록 Amazon Redshift 클러스터에 자동 스냅샷이 있는지 확인하세요. 클러스터에 자동 스냅샷이 사용되면 Redshift는 정기적으로 해당 클러스터의 스냅샷을 생성합니다. 기본적으로 Redshift는 8시간마다 또는 각 노드당 5GB의 데이터 변경이 있을 때마다 둘 중 먼저 발생하는 시점을 기준으로 스냅샷을 생성합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.IX	주기적 테스트를 통한 데이터 백업 준비	backup-plan-min-frequency-and-min-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 계획이 최소 빈도와 보존으로 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 사용하면 requiredFrequencyValue(Config 기본값: 1), requiredRetentionDays(Config 기본값: 35) 및 requiredFrequencyUnit(Config 기본값: days) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

제어 ID	제어 설명	AWS 구성 규칙	지침
8.IX	주기적 테스트를 통한 데이터 백업 준비	backup-recovery-point-manual-deletion-disabled	AWS Backup 복구 시점에 복구 시점 삭제를 방지하는 리소스 기반 정책이 연결되어 있는지 확인합니다. 리소스 기반 정책을 사용하여 복구 시점의 삭제를 방지하면 우발적 또는 의도적인 삭제를 방지하는 데 도움이 될 수 있습니다.
8.IX	주기적 테스트를 통한 데이터 백업 준비	backup-recovery-point-minimum-retention-check	데이터 백업 프로세스에 도움이 되도록 AWS 백업 복구 시점에 최소 보존 기간이 설정되어 있는지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다. 이 규칙을 통해 requiredRetentionDays(Config 기본값: 35) 파라미터를 설정할 수 있습니다. 실제 값은 조직의 요구 사항을 반영해야 합니다.

템플릿

템플릿은 GitHub: RBI MD-ITF 운영 모범 사례에서 확인할 수 있습니다.

보안, 자격 증명 및 규정 준수 서비스 운영 모범 사례

이 적합성 팩에는 보안, 자격 증명 및 규정 준수 서비스에 기반한 AWS Config 규칙이 포함되어 있습니다. 자세한 내용은 의 보안, 자격 증명 및 규정 준수를 AWS 참조하세요. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: AWS의 보안, 자격 증명 및 규정 준수 운영 모범 사례에서 확인할 수 있습니다.

서버리스 운영 모범 사례

이 적합성 팩에는 Serverless 솔루션을 기반으로 하는 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 서버리스 운영 모범 사례에서 확인할 수 있습니다.

스토리지 서비스 운영 모범 사례

이 적합성 팩에는 스토리지 서비스에 기반한 AWS Config 규칙이 포함되어 있습니다. 자세한 내용은 Cloud Storage on AWS을 참조하세요. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 스토리지 서비스 운영 모범 사례에서 확인할 수 있습니다.

SWIFT CSP 운영 모범 사례

적합성 팩은 관리형 또는 사용자 지정 AWS Config 규칙 및 AWS Config 문제 해결 작업을 사용하여 보안, 운영 또는 비용 최적화 거버넌스 검사를 생성할 수 있도록 설계된 범용 규정 준수 프레임워크를 제공합니다. 샘플 템플릿인 적합성 팩은 특정 거버넌스 또는 규정 준수 표준을 완벽하게 준수하도록 설계되지 않았습니다. 사용자는 서비스 이용이 관련 법률 및 규제 요구 사항을 충족하는지 여부를 스스로 평가할 책임이 있습니다.

다음은 SWIFT 고객 보안 프로그램(CSP)과 관리형 AWS Config 규칙 간의 샘플 매핑입니다. 각 AWS Config 규칙은 특정 AWS 리소스에 적용되며 하나 이상의 SWIFT CSP 제어와 관련이 있습니다. SWIFT CSP 제어는 여러 AWS Config 규칙과 관련될 수 있습니다. 이러한 매핑과 관련된 자세한 내용 및 지침은 아래 표를 참조하세요.

제어 ID	AWS 구성 규칙	지침
1.1	ec2-instance-managed-by-systems-manager	AWS Systems Manager를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하면 조직 내 소프트웨어 플랫폼 및 애플리케이션의 인벤토리를 생성할 수 있습니다. AWS Systems Manager를 사용하여 세부 시스템 구성, 운영 체제 패치 수준, 서비스 이름 및 유형, 소프트웨어 설치, 애플리케이션 이름, 게시자 및 버전, 환경에 대한 기타 세부 정보를 제공합니다.
1.1	ec2-instance-no-public-ip	Amazon Elastic Compute AWS Cloud(Amazon EC2) 인스턴스에 공개적으로 액세스할 수 없도록 하여 클라우드에 대한 액세스를 관리합니다. Amazon EC2 인스턴스에는 민감한 정보가 포함될 수 있으며 이러한 계정에는 액세스 제어가 필요합니다.
1.1	ec2-no-amazon-key-pair	이 규칙은 실행 중인 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스가 Amazon 키 페어를 사용하여 시작되는지 확인합니다. 이렇게 하면 보

제어 ID	AWS 구성 규칙	지침
		안 인증이 손상될 위험을 줄이는 데 도움이 될 수 있습니다. 키 페어가 없는 Amazon EC2 인스턴스는 AWS 콘솔에서 세션 관리자 또는 브라우저 기반 SSH 연결을 사용하여 계속 액세스할 수 있습니다.
1.1	ec2-instances-in-vpc	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 Amazon Virtual Private Cloud(VPC) 내에 배포하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결 없이 Amazon VPC 내부에서 인스턴스와 다른 서비스 간에 보안 통신이 가능합니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. Amazon EC2 인스턴스를 Amazon VPC에 할당하여 액세스를 적절하게 관리합니다.

제어 ID	AWS 구성 규칙	지침
1.1	vpc-default-security-group-closed	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스로 들어오는 네트워크 트래픽과 나가는 네트워크 트래픽을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 기본 보안 그룹의 모든 트래픽을 제한하면 AWS 리소스에 대한 원격 액세스를 제한하는 데 도움이 됩니다.
1.1	vpc-network-acl-unused-check	이 규칙은 Amazon Virtual Private Cloud(VPC) 네트워크 액세스 제어 목록이 사용되도록 합니다. 사용하지 않는 네트워크 액세스 제어 목록을 모니터링하면 환경의 정확한 인벤토리와 관리에 도움이 될 수 있습니다.
1.1	vpc-sg-open-only-to-authorized-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 인터넷(0.0.0.0/0)에서 보안 그룹 내 리소스에 대한 액세스를 제한함으로써 내부 시스템에 대한 원격 액세스를 제어할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1.2	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management(IAM)를 사용하면 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한과 통합하여 정책이 모든 AWS Key Management Service 키에 차단된 작업을 포함하지 못하도록 제한할 수 있습니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
1.2	iam-group-has-users-check	AWS Identity and Access Management(IAM)는 IAM 그룹에 최소 한 명의 사용자가 있는지 확인하여 최소 권한 및 업무 분리 원칙을 액세스 권한 및 권한 부여와 통합하는 데 도움이 될 수 있습니다. 관련 권한 또는 직무에 따라 사용자를 그룹에 배치하는 것은 최소 권한을 통합하는 한 가지 방법입니다.

제어 ID	AWS 구성 규칙	지침
1.2	iam-inline-policy-blocked-kms-actions	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 모든 AWS Key Management Service 키에 대해 차단된 작업을 허용하는 인라인 정책이 없는지 확인합니다. AWS 는 인라인 정책 대신 관리형 정책을 사용하도록 권장합니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다. 이 규칙을 사용하면 blockedActionsPatterns 파라미터를 설정할 수 있습니다. (AWS 기본 보안 모범 사례 값: kms:Decrypt, kms:ReEncryptFrom). 실제 값은 조직의 정책을 반영해야 합니다.
1.2	iam-no-inline-policy-check	AWS Identity and Access Management(IAM) 사용자, IAM 역할 또는 IAM 그룹에 시스템 및 자산에 대한 액세스를 제어하는 인라인 정책이 없는지 확인합니다. 인라인 정책 대신 관리형 정책을 사용하는 것이 AWS 좋습니다. 관리형 정책을 사용하면 재사용, 버전 관리, 롤백 및 권한 위임 관리가 가능합니다.

제어 ID	AWS 구성 규칙	지침
1.2	iam-user-no-policies-check	이 규칙은 AWS ID 및 액세스 관리(IAM) 정책이 그룹 또는 역할에만 연결되어 시스템 및 자산에 대한 액세스를 제어하도록 합니다. 그룹 또는 역할 수준에서 권한을 할당하면 ID가 과도한 권한을 받거나 보유할 기회를 줄이는 데 도움이 됩니다.
1.2	restricted-ssh	Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹은 AWS 리소스에 대한 네트워크 트래픽의 수신 및 송신을 상태 저장 필터링하여 네트워크 액세스를 관리하는 데 도움이 될 수 있습니다. 리소스의 0.0.0.0/0에서 포트 22로 수신(또는 원격) 트래픽을 허용하지 않으면 원격 액세스를 제한하는 데 도움이 됩니다.
1.2	nacl-no-unlimitted-ssh-rdp	포트 22(SSH) 및 포트 3389(RDP)와 같은 네트워크 액세스 제어 목록(NACL)에 포함된 원격 서버 관리 포트에 대한 액세스는 공개적으로 액세스할 수 없도록 해야 합니다. 그렇지 않으면 VPC 내 리소스에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

제어 ID	AWS 구성 규칙	지침
1.2	s3-bucket-acl-prohibited	이 규칙은 액세스 제어 목록(ACL)이 Amazon S3 버킷의 액세스 제어에 사용되는지 확인합니다. ACLs은 AWS Identity and Access Managemen t(IAM) 이전의 Amazon S3 버킷에 대한 레거시 액세스 제어 메커니즘입니다. ACL 대신 IAM 정책 또는 S3 버킷 정책을 사용하여 S3 버킷에 대한 액세스를 보다 쉽게 관리하는 것은 모범 사례입니다.
1.2	s3-bucket-logging-enabled	Amazon Simple Storage Service(S3) 서버 액세스 로깅은 네트워크에 잠재적인 사이버 보안 이벤트가 있는지 모니터링하는 방법을 제공합니다. 이벤트는 Amazon S3 버킷에 대해 이루어진 요청에 대한 상세한 레코드를 캡처하여 모니터링됩니다. 각 액세스 로그 레코드는 단일 액세스 요청에 관한 세부 정보를 제공합니다. 세부 정보에는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태, 오류 코드(해당하는 경우)가 포함됩니다.

제어 ID	AWS 구성 규칙	지침
1.2	s3-bucket-policy-grantee-check	s3_ bucket_policy_grantee_check를 활성화하여 AWS 클라우드에 대한 액세스를 관리합니다. 이 규칙은 Amazon S3 버킷에서 부여한 액세스가 사용자가 제공하는 AWS 보안 주체, 연합 사용자, 서비스 보안 주체, IP 주소 또는 Amazon Virtual Private Cloud(Amazon VPC) IDs에 의해 제한되는지 확인합니다.
1.2	sns-topic-message-delivery-notification-enabled	환경의 로깅 요구 사항을 지원하려면 Amazon Simple Notification Service(SNS) 주제에 대해 전송 상태 알림을 활성화해야 합니다. 메시지 전송 상태를 기록하면 메시지가 Amazon SNS 엔드포인트로 전송되었는지 확인하고, Amazon SNS 엔드포인트에서 Amazon SNS로 전송된 응답을 식별하고, 메시지 체류 시간(게시 타임스탬프와 Amazon SNS 엔드포인트로 전달하기 직전 사이의 시간)을 결정하는 등 운영 인사이트를 확장할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
1.4	internet-gateway-authorized-vpc-only	인터넷 게이트웨이가 승인된 Amazon Virtual Private AWS Cloud(Amazon VPC)에만 연결되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. Amazon Virtual Private Cloud 인터넷 게이트웨이를 사용하면 Amazon VPC와 주고받는 양방향 인터넷 액세스가 가능하므로 Amazon VPC 리소스에 대한 무단 액세스가 발생할 수 있습니다.
1.4	restricted-common-ports	Amazon Elastic Compute AWS Cloud(Amazon EC2) 보안 그룹에서 공통 포트가 제한되도록 하여 클라우드의 리소스에 대한 액세스를 관리합니다. 포트 액세스를 신뢰할 수 있는 소스로 제한하지 않으면 시스템의 가용성, 무결성 및 기밀성에 대한 공격이 발생할 수 있습니다. 이 규칙을 사용하면 blockedPort1 ~ blockedPort5 파라미터를 선택적으로 설정할 수 있습니다(Config 기본값: 20,21,3389,3306,4333). 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
1.4	lambda-function-public-access-prohibited	AWS Lambda 함수에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 퍼블릭 액세스는 잠재적으로 리소스 가용성을 저하시킬 수 있습니다.
1.4	s3-account-level-public-access-blocks-periodic	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 퍼블릭 액세스를 방지하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다. 이 규칙을 사용하면 ignorePublicAcls(Config 기본값: True), blockPublicPolicy(Config 기본값: True), blockPublicAcls(Config 기본값: True) 및 restrictPublicBuckets 파라미터(Config 기본값: True)를 선택적으로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
1.4	s3-bucket-level-public-access-prohibited	Amazon Simple Storage Service(Amazon S3) 버킷에 공개적으로 액세스할 수 없도록 하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 이 규칙은 버킷 수준에서 퍼블릭 액세스를 차단하여 권한이 없는 원격 사용자로부터 민감한 데이터를 안전하게 보호하는 데 도움이 됩니다.
1.4	s3-bucket-public-read-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.
1.4	s3-bucket-public-write-prohibited	승인된 사용자, 프로세스 및 디바이스만 Amazon Simple Storage Service(Amazon S3) 버킷에 액세스할 수 있도록 허용하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 액세스 관리는 데이터 분류와 일치해야 합니다.

제어 ID	AWS 구성 규칙	지침
1.4	ssm-document-not-public	AWS Systems Manager(SSM) 문서는 SSM 문서에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개되지 않아야 합니다. 퍼블릭 SSM 문서를 통해 계정, 리소스 및 내부 프로세스에 관한 정보가 노출될 수 있습니다.
2.3	ec2-imdsv2-check	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 메타데이터의 액세스 및 제어를 위해 인스턴스 메타데이터 서비스 버전 2(IMDSv2) 메서드가 활성화되어 있는지 확인합니다. IMDSv2 메서드는 세션 기반 제어를 사용합니다. IMDSv2를 사용하면 제어를 구현하여 인스턴스 메타데이터 변경을 제한할 수 있습니다.
2.3	ec2-instance-multiple-eni-check	이 규칙은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 ENI가 여러 개 있는지 확인합니다. ENI가 여러 개 있으면 이중 홈 인스턴스, 즉 서브넷이 여러 개 있는 인스턴스가 발생할 수 있습니다. 이로 인해 네트워크 보안이 복잡해지고 의도하지 않은 네트워크 경로와 액세스가 발생할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.3	ec2-token-hop-limit-check	인스턴스 메타데이터 서비스(IMDS) HTTP PUT 응답이 Amazon Elastic Compute Cloud(Amazon EC2)인스턴스로 제한되는지 확인합니다. IMDSv2를 사용하면 메타데이터 응답 홉 제한이 1(Config 기본값)로 설정되어 있기 때문에 기본적으로 비밀 토큰이 포함된 PUT 응답은 인스턴스 외부로 이동할 수 없습니다. 이 값이 1보다 크면 토큰은 EC2 인스턴스에서 나갈 수 있습니다.
2.3	ec2-volume-inuse-check	이 규칙은 인스턴스 종료 시 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 Amazon Elastic Block Store 볼륨이 삭제 대상으로 표시되도록 합니다. 연결된 인스턴스가 종료될 때 Amazon EBS 볼륨이 삭제되지 않으면 최소 기능 개념을 위반할 수 있습니다.
2.3	account-part-of-organizations	AWS Organizations AWS 계정 내 중앙 집중식 관리는 계정이 규정을 준수하도록 하는 데 도움이 됩니다. 중앙 집중식 계정 거버넌스가 없으면 계정 구성이 일관되지 않아 리소스와 민감한 데이터가 노출될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.3	lambda-inside-vpc	Amazon Virtual Private Cloud(Amazon VPC) 내에 AWS Lambda 함수를 배포하여 Amazon VPC 내의 함수와 다른 서비스 간의 안전한 통신을 보장합니다. 이 구성을 사용하면 인터넷 게이트웨이, NAT 디바이스 또는 VPN 연결이 필요하지 않습니다. 모든 트래픽은 AWS 클라우드 내에서 안전하게 유지됩니다. 논리적 격리로 인해 퍼블릭 엔드포인트를 사용할 때에 비해, Amazon VPC에 상주하는 도메인에는 보안 계층이 하나 추가됩니다. 액세스를 올바르게 관리하려면 AWS Lammbda 함수를 VPC에 할당해야 합니다.
2.3	kms-cmk-not-scheduled-for-deletion	저장 데이터를 보호하기 위해 필요한 고객 마스터 키(CMKs)가 AWS Key Management Service(AWS KMS)에서 삭제되도록 예약되지 않았는지 확인합니다. 때때로 키 삭제가 필요하기 때문에 이 규칙은 실수로 키가 예약된 경우 삭제가 예약된 모든 키를 확인하는 데 도움을 줄 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.3	s3-bucket-versioning-enabled	Amazon Simple Storage Service(S3) 버킷 버전 관리를 사용하면 동일한 Amazon S3 버킷 내에 객체의 여러 변형을 보유할 수 있습니다. 버전 관리를 사용하여 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원합니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.
2.3	secretsmanager-secret-unused	AWS Secrets Manager에 미사용 자격 증명이 있는 경우 자격 증명을 비활성화 및/또는 제거해야 합니다. 최소 권한 원칙을 위반할 수 있습니다. 이 규칙을 사용하면 값을 unusedForDays(Config 기본값: 90)로 설정할 수 있습니다. 실제 값은 조직의 정책을 반영해야 합니다.
2.5A	ebs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic Block Store(Amazon EBS) 볼륨이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 사용하는 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구사항을 충족할 수 있습니다.

제어 ID	AWS 구성 규칙	지침
2.5A	ec2-ebs-encryption-by-default	저장 데이터를 보호하려면Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화해야 합니다. 이러한 볼륨에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
2.5A	efs-encrypted-check	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic File System(EFS)에 대해 암호화가 활성화되어 있는지 확인합니다.
2.5A	efs-in-backup-plan	데이터 백업 프로세스에 도움이 되도록 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS 백업 계획의 일부인지 확인합니다. AWS 백업은 정책 기반 백업 솔루션을 갖춘 완전 관리형 백업 서비스입니다. 이 솔루션을 사용하면 백업 관리를 단순화하고 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족할 수 있습니다.
2.5A	encrypted-volumes	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Elastic Block Store(Amazon EBS)에 대해 암호화가 활성화되어 있는지 확인합니다.

제어 ID	AWS 구성 규칙	지침
2.5A	kinesis-stream-encrypted	민감한 데이터가 존재할 수 있으므로 저장 데이터를 보호하는 데 도움이 되도록 Amazon Kinesis Streams에 암호화가 활성화되어 있는지 확인합니다.
2.5A	s3-bucket-server-side-encryption-enabled	저장 데이터를 보호하려면 Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 암호화를 활성화하여 해당 데이터를 보호합니다.
2.5A	s3-default-encryption-kms	Amazon Simple Storage Service(S3) 버킷에 대해 암호화가 활성화되어 있는지 확인합니다. Amazon S3 버킷에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
2.5A	sns-encrypted-kms	저장 데이터를 보호하려면 Amazon Simple Notification Service(Amazon SNS) 주제에 AWS Key Management Service(AWS KMS)를 사용한 암호화가 필요한지 확인합니다. 게시된 메시지에 민감한 데이터가 저장될 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.

제어 ID	AWS 구성 규칙	지침
4.1	iam-password-policy	ID 및 보안 인증 정보는 조직의 IAM 암호 정책을 기반으로 발급, 관리 및 검증됩니다. NIST SP 800-63 및 암호 강도에 대한 AWS 기본 보안 모범 사례 표준에 명시된 요구 사항을 충족하거나 초과합니다. 이 규칙을 사용하면 옵션으로 RequireUppercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireLowercaseCharacters(AWS 기본 보안 모범 사례 값: true), RequireSymbols(AWS 기본 보안 모범 사례 값: true), RequireNumbers(AWS 기본 보안 모범 사례 값: true), MinimumPasswordLength(AWS 기본 보안 모범 사례 값: 14), PasswordReusePrevention(AWS 기본 보안 모범 사례 값: 24), 및 MaxPasswordAge(AWS 기본 보안 모범 사례 값: 90)를 사용합니다. 실제 값은 조직의 정책을 반영해야 합니다.

제어 ID	AWS 구성 규칙	지침
4.1	access-keys-rotated	조직 정책에서 지정한 대로 IAM 액세스 키가 교체되도록 하여 승인된 디바이스, 사용자 및 프로세스에 대한 보안 인증을 감사합니다. 정기적인 일정에 따라 액세스 키를 변경하는 것이 보안 모범 사례입니다. 이렇게 하면 액세스 키가 활성화되는 기간이 단축되고 키가 손상될 경우 비즈니스에 미치는 영향을 줄일 수 있습니다. 이 규칙에는 액세스 키 교체 값이 필요합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
4.2	iam-user-mfa-enabled	AWS 클라우드의 리소스에 대한 액세스를 제한하려면이 규칙을 활성화합니다. 이 규칙은 모든 사용자에 대해 다중 인증(MFA)이 활성화되도록 합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하여 계정 보안 침해 사고를 줄이세요.

제어 ID	AWS 구성 규칙	지침
4.2	mfa-enabled-for-iam-console-access	콘솔 암호가 있는 모든 AWS Identity and Access Management(IAM) 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. MFA를 통해 로그인 보안 인증 외에 보호 계층이 한 단계 더 추가됩니다. 사용자에게 MFA를 요구하면 계정이 침해되는 사고를 줄이고 승인되지 않은 사용자가 민감한 데이터에 액세스하는 것을 방지할 수 있습니다.
4.2	root-account-hardware-mfa-enabled	루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.

제어 ID	AWS 구성 규칙	지침
4.2	root-account-mfa-enabled	루트 사용자에 대해 MFA가 활성화되어 있는지 확인하여 AWS 클라우드의 리소스에 대한 액세스를 관리합니다. 루트 사용자는 권한이 가장 많은 AWS 계정사용자입니다. MFA는 로그인 보안 인증에 보호 계층을 한 단계 더 추가합니다. 루트 사용자에게 MFA를 요구하면 손상된 인시던트를 줄일 수 있습니다 AWS 계정.
5.1	ec2-instance-profile-attached	EC2 인스턴스 프로파일은 EC2 인스턴스에 IAM 역할을 전달합니다. 인스턴스 프로파일을 인스턴스에 연결하면 최소 권한 및 권한 관리에 도움이 될 수 있습니다.
5.1	iam-policy-no-statements-with-full-access	IAM 작업을 필요한 작업으로만 제한해야 합니다. 작업을 완료하는 데 필요한 것보다 더 많은 권한을 갖도록 허용하는 것은 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
5.1	iam-root-access-key-check	루트 사용자에게 AWS Identity and Access Managemen t(IAM) 역할에 연결된 액세스 키가 없는지 확인하여 시스템 및 자산에 대한 액세스를 제어할 수 있습니다. 루트 액세스 키가 삭제되었는지 확인하세요. 대신 역할 기반 AWS 계정 를 생성하고 사용하여 최소 기능의 원칙을 통합합니다.
5.1	iam-user-group-membership-check	AWS Identity and Access Management(IAM)는 사용자가 하나 이상의 그룹의 멤버가 되도록 하여 액세스 권한 및 권한 부여를 제한하는 데 도움이 될 수 있습니다. 사용자에게 작업을 완료하는 데 필요한 것보다 더 많은 권한을 허용하면 최소 권한 및 업무 분리 원칙에 위배될 수 있습니다.

제어 ID	AWS 구성 규칙	지침
5.1	iam-user-unused-credentials-check	AWS Identity and Access Management(IAM)는 지정된 기간 동안 사용되지 않는 IAM 암호 및 액세스 키를 확인하여 액세스 권한 및 권한 부여를 지원합니다. 이러한 미사용 보안 인증 정보가 발견되면 최소 권한의 원칙에 위배될 수 있으므로 해당 보안 인증 정보를 비활성화 및/또는 제거해야 합니다. 이 규칙을 사용하려면 maxCredentialUsageAge 값을 설정해야 합니다(Config 기본값: 90). 실제 값은 조직의 정책을 반영해야 합니다.
5.4	secretsmanager-rotation-enabled-check	이 규칙은 AWS Secrets Manager 보안 암호에 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.
5.4	secretsmanager-scheduled-rotation-success-check	이 규칙은 AWS Secrets Manager 보안 암호가 교체 일정에 따라 성공적으로 교체되도록 합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다.

제어 ID	AWS 구성 규칙	지침
5.4	secretsmanager-secret-periodic-rotation	이 규칙은 AWS Secrets Manager 보안 암호에 주기적 교체가 활성화되어 있는지 확인합니다. 정기적으로 암호를 교체하면 암호가 활성화되는 기간을 단축할 수 있으며, 암호가 침해될 경우 비즈니스에 미치는 영향을 잠재적으로 줄일 수 있습니다. 기본값은 90일입니다.
5.4	secretsmanager-using-cmk	저장 데이터를 보호하기 위해 AWS Secrets Manager 보안 암호에 AWS 대해 Key Management Service(AWS KMS)를 사용한 암호화가 활성화되어 있는지 확인합니다. Secrets Manager 암호에 저장 중 민감한 데이터가 존재할 수 있으므로 저장 중 암호화를 활성화하여 해당 데이터를 보호합니다.
6.4	ec2-instance-detailed-monitoring-enabled	이 규칙을 활성화하면 Amazon EC2 콘솔에서 인스턴스에 대한 1분 모니터링 그래프를 표시하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 모니터링을 개선하는 데 도움이 됩니다.
6.4	cloudwatch-log-group-encrypted	민감한 저장 데이터를 보호하려면 Amazon CloudWatch 로그 그룹에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
6.4	cloud-trail-cloud-watch-logs-enabled	Amazon CloudWatch를 사용하여 로그 이벤트 활동을 중앙에서 수집하고 관리합니다. AWS CloudTrail 데이터를 포함하면 내 API 호출 활동에 대한 세부 정보가 제공됩니다 AWS 계정.
6.4	cloudtrail-enabled	AWS CloudTrail은 AWS Management Console 작업 및 API 호출을 기록하여 거부 방지에 도움이 될 수 있습니다. AWS 서비스를 호출 AWS 계정 한 사용자 및 , 호출이 생성된 소스 IP 주소, 호출 타이밍을 식별할 수 있습니다. 캡처된 데이터의 세부 정보는 AWS CloudTrail 레코드 콘텐츠에서 확인할 수 있습니다.
6.4	cloud-trail-encryption-enabled	민감한 데이터가 존재할 수 있고 저장 데이터를 보호하는 데 도움이 될 수 있으므로 AWS CloudTrail 추적에 암호화가 활성화되어 있는지 확인하세요.

제어 ID	AWS 구성 규칙	지침
6.4	cloud-trail-log-file-validation-enabled	AWS CloudTrail 로그 파일 검증을 활용하여 CloudTrail 로그의 무결성을 확인합니다. 로그 파일 검증을 통해 CloudTrail이 로그 파일을 전달한 후 로그 파일이 수정, 삭제 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)으로 구축되었습니다. 따라서 CloudTrail 로그 파일의 수정, 삭제 또는 위조가 감지되지 않는 것이 계산상 불가능합니다.
6.4	ec2-stopped-instance	이 규칙을 활성화하면 조직의 표준에 따라 Amazon EC2 인스턴스가 허용된 일수를 초과하여 중지되었는지 확인하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 기본 구성을 쉽게 수행할 수 있습니다.
6.4	vpc-flow-logs-enabled	VPC 흐름 로그는 Amazon Virtual Private Cloud(VPC)의 네트워크 인터페이스에서 들어오고 나가는 IP 트래픽에 관한 정보의 자세한 기록을 제공합니다. 기본적으로 이 흐름 로그 레코드에는 소스, 대상, 프로토콜 등 IP 흐름의 다양한 구성 요소에 대한 값이 포함됩니다.

제어 ID	AWS 구성 규칙	지침
6.5A	guardduty-enabled-centralized	Amazon GuardDuty는 위협 인텔리전스 피드를 사용하여 잠재적인 사이버 보안 이벤트를 모니터링하고 탐지하는 데 도움이 될 수 있습니다. 여기에는 AWS 클라우드 환경 내에서 예상치 못한, 승인되지 않은, 악의적인 활동을 식별하기 위한 악성 IPs 및 기계 학습 목록이 포함됩니다.
6.5A	securityhub-enabled	AWS Security Hub는 권한이 없는 직원, 연결, 디바이스 및 소프트웨어를 모니터링하는 데 도움이 됩니다. AWS Security Hub는 여러 AWS 서비스의 보안 알림 또는 조사 결과를 집계, 구성 및 우선 순위를 지정합니다. 이러한 서비스 중에는 Amazon Security Hub, Amazon Inspector, Amazon Macie, IAM(AWS Identity and Access Managemen t) Access Analyzer, AWS Firewall Manager 및 AWS 파트너 솔루션이 있습니다.

템플릿

템플릿은 GitHub: SWIFT CSP 운영 모범 사례에서 확인할 수 있습니다.

Amazon Elastic Container Service(Amazon ECS) 보안 모범 사례

이 적합성 팩에는 Amazon ECS 기반 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: Amazon ECS 보안 모범 사례에서 확인할 수 있습니다.

Amazon Elastic File System(Amazon EFS) 보안 모범 사례

이 적합성 팩에는 Amazon EFS 기반 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: Amazon EFS 보안 모범 사례에서 확인할 수 있습니다.

Amazon Elastic Kubernetes Service(Amazon EKS) 보안 모범 사례

이 적합성 팩에는 Amazon EKS 기반 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: Amazon EKS 보안 모범 사례에서 확인할 수 있습니다.

Amazon CloudFront 보안 모범 사례

이 적합성 팩에는 Amazon CloudFront 기반 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: Amazon CloudFront 보안 모범 사례에서 확인할 수 있습니다.

Amazon OpenSearch Service 보안 모범 사례

이 적합성 팩에는 Amazon OpenSearch Service 기반 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: Amazon OpenSearch Service 보안 모범 사례에서 확인할 수 있습니다.

Amazon Redshift 보안 모범 사례

이 적합성 팩에는 Amazon Redshift 기반 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: Amazon Redshift 보안 모범 사례에서 확인할 수 있습니다.

Amazon Relational Database Service(RDS) 보안 모범 사례

이 적합성 팩에는 Amazon RDS 기반 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: Amazon RDS 보안 모범 사례에서 확인할 수 있습니다.

AWS Auto Scaling보안 모범 사례

이 적합성 팩에는 기반 AWS Config 규칙이 포함되어 있습니다 AWS Auto Scaling. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 보안 모범 사례에서 사용할 수 있습니다 AWS Auto Scaling.

AWS CloudTrail보안 모범 사례

이 적합성 팩에는 기반 AWS Config 규칙이 포함되어 있습니다 AWS CloudTrail. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 보안 모범 사례에서 사용할 수 있습니다 AWS CloudTrail.

AWS CodeBuild보안 모범 사례

이 적합성 팩에는 기반 AWS Config 규칙이 포함되어 있습니다 AWS CodeBuild. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 보안 모범 사례에서 사용할 수 있습니다 AWS CodeBuild.

Amazon ECR 보안 모범 사례

이 적합성 팩에는 Amazon Elastic Container Registry(Amazon ECR) 기반 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: Amazon ECR 보안 모범 사례에서 확인할 수 있습니다.

AWS Lambda보안 모범 사례

이 적합성 팩에는 기반 AWS Config 규칙이 포함되어 있습니다 AWS Lambda. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 보안 모범 사례에서 사용할 수 있습니다 AWS Lambda.

AWS Network Firewall보안 모범 사례

이 적합성 팩에는 기반 AWS Config 규칙이 포함되어 있습니다 AWS Network Firewall. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 보안 모범 사례에서 사용할 수 있습니다 AWS Network Firewall.

Amazon SageMaker AI의 보안 모범 사례

이 적합성 팩에는 Amazon SageMaker AI 기반 AWS Config 규칙이 포함되어 있습니다. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: Amazon SageMaker AI의 보안 모범 사례에서 사용할 수 있습니다.

AWS Secrets Manager보안 모범 사례

이 적합성 팩에는 기반 AWS Config 규칙이 포함되어 있습니다 AWS Secrets Manager. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 보안 모범 사례에서 사용할 수 있습니다 AWS Secrets Manager.

AWS WAF보안 모범 사례

이 적합성 팩에는 기반 AWS Config 규칙이 포함되어 있습니다 AWS WAF. 에서 지원하는 모든 관리형 규칙 목록은 관리형 규칙 목록을 AWS Config참조하세요. AWS Config

필수 파라미터의 이름 및 설명은 다음 템플릿의 `Parameters` 섹션을 참조하세요.

템플릿은 GitHub: 보안 모범 사례에서 사용할 수 있습니다 AWS WAF.

문제 해결 작업이 포함된 템플릿의 예

문제 해결이 포함된 Amazon DynamoDB 운영 모범 사례

템플릿은 GitHub: 문제 해결이 포함된 Amazon DynamoDB 운영 모범 사례에서 확인할 수 있습니다.

문제 해결이 포함된 Amazon S3 운영 모범 사례

템플릿은 GitHub: 문제 해결이 포함된 Amazon S3 운영 모범 사례에서 확인할 수 있습니다.

템플릿 구조 페이지에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 템플릿 구조를 참조하세요.

용 사용자 지정 적합성 팩에 대한 템플릿 생성 AWS Config

사용자 지정 적합성 팩은 계정과 AWS 리전 또는의 조직 전체에 함께 배포할 수 있는 고유한 AWS Config 규칙 및 문제 해결 작업 모음입니다 AWS Organizations.

사용자 지정 적합성 팩을 생성하려면 다음 템플릿 사용자 지정 섹션의 단계에 따라 작업하려는 AWS Config 관리형 규칙 또는 AWS Config 사용자 지정 규칙의 목록이 포함된 YAML 파일을 작성합니다.

주제

- 용어

- 템플릿 사용자 지정

용어

AWS Config 관리형 규칙은에서 소유한 사전 정의된 규칙입니다 AWS Config.

AWS Config 사용자 지정 규칙은 처음부터 생성하는 규칙입니다.

AWS Config 사용자 지정 규칙을 생성하는 방법에는 두 가지가 있습니다. Lambda 함수(AWS Lambda 개발자 안내서)와 Guard(Guard GitHub 리포지토리)를 사용하는 policy-as-code로 AWS Lambda 생성된 AWS Config 사용자 지정 규칙을 AWS Config 사용자 지정 Lambda 규칙이라고 하고 Guard로 생성된 AWS Config 사용자 지정 규칙을 AWS Config 사용자 지정 정책 규칙이라고 합니다.

템플릿 사용자 지정

YAML 파일 작성

YAML 파일을 작성하려면 텍스트 편집기를 열고 파일을 .yaml로 저장합니다.

> **Note**
>
> 파일에는 파라미터 및 리소스 섹션이 포함됩니다.

파라미터

YAML 파일의 `Parameters` 섹션은 `Resources` 섹션 뒷부분에서 추가할 규칙 세트의 AWS Config 규칙 파라미터에 대한 것입니다. 다음 코드 블록을 복사하여 YAML 파일에 붙여넣고 필요에 따라 사용자 지정하고 각 규칙 파라미터에 대해 반복하여 `Parameters` 섹션을 생성합니다.

```
Parameters:
    NameOfRuleParamNameOfRuleParameter:
        Default: Parameter value
        Type: Type
    ...
```

예시:

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
```

```
        Default: '14'
        Type: String
```

> **Note**
>
> AWS Config 규칙을 선택하여 사용자 지정 적합성 팩을 빌드할 때 AWS Config 규칙에 대해 평가될 리소스가 계정 내에 프로비저닝되었는지 확인합니다.

1. `Parameters:` 뒤에 있는 파라미터 섹션의 첫 번째 줄은 *`NameOfRule`* + Param + *`NameOfRuleParameter`* 문자열입니다.

   a. *`NameOfRule`*을 규칙에 대해 생성한 일관된 이름으로 바꿉니다. 예를 들면 iam-password-policy 규칙의 IamPasswordPolicy입니다.

   b. 유형 `Param`

   c. 그런 다음 *`NameOfRuleParameter`*를 특정 규칙의 규칙 파라미터의 이름으로 바꿉니다. AWS Config 관리형 규칙의 경우 규칙 파라미터의 이름은 관리형 규칙 목록에 AWS Config 있습니다(예: MinimumPasswordLength는 iam-password-policy 규칙의 규칙 파라미터 이름). AWS Config 사용자 지정 규칙의 경우 규칙 파라미터의 이름은 규칙을 생성할 때 선택한 이름입니다.

2. AWS Config 관리형 규칙을 사용하는 경우 관리형 AWS Config 규칙 목록에서 적절한 규칙을 찾아 특정 규칙의 `Default` 및에 `Type` 대해 허용되는 값을 알 수 있습니다. AWS Config 사용자 지정 규칙의 경우 규칙을 생성할 때 선택한 값을 사용합니다.

   > **Note**
   >
   > 각 파라미터에 대해 `Type`을 지정해야 합니다. `Type`은 '문자열', 'int', 'double', 'CSV', '부울', 'StringMap' 중 하나일 수 있습니다.

리소스

이 `Resources` 섹션에는 사용자 지정 적합성 팩에 추가되는 규칙이 나열되어 있습니다. `Parameters` 섹션 바로 아래에 다음 `Resources` 블록을 추가한 다음 필요에 따라 사용자 지정하고 각 규칙에 대해 반복합니다. 사양에 대한 자세한 내용은 AWS::Config::ConfigRule을 참조하세요.

```
Resources:
```

```
    NameOfRule:
        Properties:
            ConfigRuleName: ActualConfigRuleName
            InputParameters:
                NameOfRuleParameter: !Ref NameOfRuleParamNameOfRuleParameter
            Source:
                Owner: Owner
                SourceIdentifier: SOURCE_IDENTIFIER
        Type: AWS::Config::ConfigRule
    ...
```

예시:

```
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
```

> **Note**
>
> 사용자 지정 적합성 팩을 빌드할 AWS Config 규칙을 선택할 때 계정 내에 프로비저닝된 AWS Config 규칙에 대해 평가할 리소스가 있는지 확인합니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.

1. *NameOfRule*을 `Parameters` 섹션에서 지정한 이름으로 바꿉니다.
2. AWS Config 관리형 규칙의 경우를 AWS Config 관리형 규칙 목록의 해당 규칙 페이지의 제목*ActualConfigRuleName*으로 바꿉니다. AWS Config 사용자 지정 규칙의 경우 규칙 생성 시 선택한 Config 규칙 이름을 사용합니다.
3. *NameOfRuleParameter*을 `Parameters` 섹션에서 사용한 이름으로 바꿉니다. 콜론 뒤에 `Parameters` 섹션에서 생성한 것과 동일한 연결 문자열인 `!Ref` + *NameOfRule* + Param + *NameOfRuleParameter*를 복사하여 붙여 넣습니다.

4. *Owner*를 적절한 값으로 변경합니다.

> **Note**
>
> AWS Config 관리형 규칙
>
> AWS Config 관리형 규칙의 경우의 값은 `Owner`입니다`AWS`.
>
> AWS Config 사용자 지정 규칙
>
> Guard로 생성된 AWS Config 사용자 지정 규칙의 경우의 값은 `Owner`입니다`CUSTOM_POLICY`. Lambda로 생성된 AWS Config 사용자 지정 규칙의 경우의 값은 `Owner`입니다`CUSTOM_LAMBDA`.

5. *SOURCE_IDENTIFIER*를 적절한 값으로 변경합니다.

> **Note**
>
> AWS Config 관리형 규칙
>
> AWS Config 관리형 규칙의 경우 AWS Config 관리형 규칙 목록에서 선택한 규칙의 링크를 따라 식별자를 복사합니다(예: access-keys-rotated 규칙의 소스 식별자는ACCESS_KEYS_ROTATED).
>
> AWS Config 사용자 지정 규칙
>
> Lambda로 생성된 AWS Config 사용자 지정 규칙의 경우 `SourceIdentifier`는와 같은 규칙 AWS Lambda 함수의 Amazon 리소스 이름(ARN)입니다`arn:aws:lambda:us-east-2:123456789012:function:`*`ActualConfigRuleName`*. Guard로 생성된 AWS Config 사용자 지정 규칙의 경우이 필드는 필요하지 않습니다.

전체적으로, 작성한 사용자 지정 적합성 팩은 다음과 비슷하게 나타나기 시작해야 합니다. 이는 iam-password-policy, access-keys-rotated, iam-user-unused-credentials-check와 같은 AWS Config 관리형 규칙을 사용하는 예입니다.

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
    AccessKeysRotatedParamMaxAccessKeyAge:
        Default: '90'
        Type: String
    IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge:
        Default: '45'
```

```
        Type: String
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
    AccessKeysRotated:
        Properties:
            ConfigRuleName: access-keys-rotated
            InputParameters:
                maxAccessKeyAge: !Ref AccessKeysRotatedParamMaxAccessKeyAge
            Source:
                Owner: AWS
                SourceIdentifier: ACCESS_KEYS_ROTATED
        Type: AWS::Config::ConfigRule
    IamUserUnusedCredentialsCheck:
        Properties:
            ConfigRuleName: iam-user-unused-credentials-check
            InputParameters:
                maxCredentialUsageAge: !Ref
 IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge
            Source:
                Owner: AWS
                SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
        Type: AWS::Config::ConfigRule
```

용 적합성 팩 배포 AWS Config

AWS Config 콘솔 또는를 사용하여 적합성 팩 AWS CLI 을 배포할 수 있습니다.

Deploy Conformance Packs (Console)

적합성 팩 페이지에서 계정에 대한 적합성 팩을 한 리전에 배포할 수 있습니다. 배포된 적합성 팩을 편집하고 삭제할 수도 있습니다.

AWS Config 샘플 템플릿 또는 자체 사용자 지정 템플릿을 사용하여 적합성 팩을 배포할 수 있습니다. 사용자 지정 적합성 팩을 생성하는 방법에 대한 지침은 사용자 지정 적합성 팩을 참조하세요.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 적합성 팩 페이지로 이동하여 적합성 팩 배포를 선택합니다.
3. 템플릿 지정 페이지에서 샘플 템플릿을 선택하거나 기존 템플릿을 사용합니다. 자세한 내용은 적합성 팩 샘플 템플릿을 참조하세요.

   - 샘플 템플릿 사용을 선택한 경우 샘플 템플릿 드롭다운 목록에서 샘플 템플릿을 선택합니다.

     각 템플릿의 콘텐츠에 대한 자세한 내용은 적합성 팩 샘플 템플릿을 참조하세요.
   - 템플릿 준비 완료를 선택하는 경우 템플릿 소스를 지정합니다. Amazon S3 URI, AWS Systems Manager 문서(SSM 문서) 또는 업로드하는 템플릿입니다.

     템플릿이 50KB를 초과하는 경우 S3 버킷에 업로드하고 해당 S3 버킷 위치를 선택합니다. 예: s3://*bucketname/prefix*.

     > **Important**
     > 적합성 팩 YAML 파일을 사용자 지정 적합성 팩을 기반으로 처음부터 생성한 경우 준비된 템플릿을 선택합니다.

4. 다음을 선택합니다.
5. 적합성 팩 세부 정보 지정 페이지에서 적합성 팩의 이름을 입력합니다.

   적합성 팩 이름은 최대 256자의 영숫자로 구성된 고유한 이름이어야 합니다. 이름에는 하이픈이 포함될 수 있지만 공백은 포함할 수 없습니다.
6. 선택 사항: 파라미터를 추가합니다.

   파라미터는 템플릿에 정의되므로 리소스를 관리하고 구성하는 데 도움이 됩니다.
7. 다음을 선택합니다.
8. 검토 및 배포 페이지에서 모든 정보를 검토합니다.

   편집을 선택하여 템플릿 세부 정보 및 적합성 팩 세부 정보를 편집할 수 있습니다.
9. 적합성 팩 배포를 선택합니다.

   AWS Config 는 적합성 팩 페이지에 적합성 팩을 적절한 상태로 표시합니다.

   적합성 팩 배포에 실패할 경우 권한을 확인하고, 사전 조건 단계를 수행했는지 확인한 후, 다시 시도하세요. 또는에 문의할 수 있습니다 AWS Support.

문제 해결이 포함된 샘플 템플릿을 사용하여 적합성 팩을 배포하려면 A. 문제 해결과 함께 적합성 팩을 사용하기 위한 사전 조건 섹션을 참조하고 위의 절차를 따르세요.

하나 이상의 AWS Config 규칙이 있는 적합성 팩을 배포하려면 섹션을 참조하세요B. 하나 이상의 사용자 지정 AWS Config 규칙과 함께 적합성 팩을 사용하기 위한 사전 조건.

Deploy Conformance Packs (AWS CLI)

1. 명령 프롬프트 또는 터미널 창을 엽니다.
2. 다음 명령 중 하나를 입력하여 **MyConformancePack**이라는 적합성 팩을 배포합니다. 템플릿 소스는 Amazon S3 URI, 업로드하는 템플릿 또는 AWS Systems Manager 문서(SSM 문서)입니다.

   Amazon S3 URI

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://amzn-s3-demo-bucket/templateName.yaml"
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

   로컬 디렉터리의 YAML 템플릿

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-body template body
   ```

   AWS Systems Manager 문서(Systems Manager 문서)

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-ssm-document-details
    DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

3. 입력을 눌러 명령을 실행합니다.

   다음과 유사한 출력 화면이 표시되어야 합니다.

   ```
   {
       "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
   MyConformancePack1/conformance-pack-ID"
   ```

```
}
```

> **Note**
>
> 적합성 팩의 YAML 템플릿을 생성하는 방법에 대한 자세한 내용은 사용자 지정 적합성 팩을 참조하세요.

에 대한 적합성 팩 편집 AWS Config

AWS Config 콘솔 또는를 사용하여 적합성 팩 AWS CLI 을 편집할 수 있습니다.

Editing Conformance Packs (Console)

1. 적합성 팩을 편집하려면 테이블에서 적합성 팩을 선택합니다.
2. 작업을 선택하고 편집을 선택합니다.
3. 적합성 팩 편집 페이지에서 템플릿 세부 정보, 샘플 템플릿, 적합성 팩 및 파라미터 섹션을 편집할 수 있습니다.

   적합성 팩의 이름은 변경할 수 없습니다.
4. Save changes(변경 사항 저장)를 선택합니다.

   적합성 팩이 AWS Config 규칙과 함께 표시됩니다.

Editing Conformance Packs (AWS CLI)

이전에 추가한 적합성 팩을 편집하는 경우 적합성 팩을 배포할 때 사용하는 것과 동일한 `PutConformancePack` 명령을 사용합니다.

1. 명령 프롬프트 또는 터미널 창을 엽니다.
2. 다음 명령 중 하나를 입력하여 **`MyConformancePack`**이라는 적합성 팩을 배포합니다. 템플릿 소스는 Amazon S3 URI, 업로드하는 템플릿 또는 AWS Systems Manager 문서(SSM 문서)입니다.

   Amazon S3 URI

   ```
   aws configservice put-conformance-pack
   ```

```
--conformance-pack-name MyConformancePack
--template-s3-uri "s3:///amzn-s3-demo-bucket/templateName.yaml"
--delivery-s3-bucket amzn-s3-demo-bucket
```

로컬 디렉터리의 YAML 템플릿

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-body template body
```

AWS Systems Manager 문서(Systems Manager 문서)

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-ssm-document-details
 DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
--delivery-s3-bucket amzn-s3-demo-bucket
```

3. 입력을 눌러 명령을 실행합니다.

   다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> 적합성 팩의 YAML 템플릿을 생성하는 방법에 대한 자세한 내용은 사용자 지정 적합성 팩을 참조하세요.

에 대한 적합성 팩 삭제 AWS Config

AWS Config 콘솔 또는를 사용하여 적합성 팩 AWS CLI 을 삭제할 수 있습니다.

고려 사항

권장 사항: 규칙을 삭제하기 전에 **`AWS::Config::ResourceCompliance`** 리소스 유형을 기록에서 제외하는 것이 좋습니다.

규칙을 삭제하면 구성 레코더 비용에 영향을 미칠 수 `AWS::Config::ResourceCompliance` 있는 에 대한 구성 항목(CIs)이 생성됩니다. 많은 수의 리소스 유형을 평가하는 규칙을 삭제하는 경우 기록된 CI의 수가 급증할 수 있습니다.

관련 비용을 방지하려면 규칙을 삭제하기 전에 `AWS::Config::ResourceCompliance` 리소스 유형에 대한 기록을 비활성화하고 규칙이 삭제된 후 기록을 다시 활성화하도록 선택할 수 있습니다.

그러나 규칙 삭제는 비동기 프로세스이므로 완료하는 데 1시간 이상 걸릴 수 있습니다. 에 대한 기록이 비활성화된 시간 동안에는 `AWS::Config::ResourceCompliance`규칙 평가가 연결된 리소스의 기록에 기록되지 않습니다.

적합성 팩을 삭제하려면

Deleting Conformance Packs (Console)

1. 적합성 팩을 삭제하려면 테이블에서 적합성 팩을 선택합니다.
2. Actions를 선택하고 삭제를 선택합니다.
3. ### # 삭제 대화 상자에서 이 적합성 팩을 영구적으로 삭제할지 확인합니다.

   > **Important**
   >
   > 이 작업은 되돌릴 수 없습니다. 적합성 팩을 삭제하면 해당 적합성 팩의 모든 AWS Config 규칙 및 문제 해결 작업이 삭제됩니다.

4. 삭제를 입력하고 삭제를선택합니다.

   적합성 팩 페이지에서 적합성 팩이 완전히 삭제될 때까지 배포 상태가 삭제 중으로 표시됩니다.

Deleting Conformance Packs (AWS CLI)

다음 명령을 입력합니다.

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

명령이 성공하면 추가 출력이 표시되지 않습니다.

> **Important**
>
> 이 작업은 되돌릴 수 없습니다. 적합성 팩을 삭제하면 해당 적합성 팩의 모든 AWS Config 규칙 및 문제 해결 작업이 삭제됩니다.

에 대한 적합성 팩의 세부 정보 및 규정 준수 정보 보기 AWS Config

> **Important**
>
> 규정 준수 상태를 정확하게 보고하려면 `AWS::Config::ResourceCompliance` 리소스 유형을 반드시 기록해야 합니다. 자세한 내용은 AWS 리소스 기록을 참조하세요.

AWS Config 콘솔 또는를 사용하여 적합성 팩 AWS CLI 을 볼 수 있습니다. AWS Config 콘솔에는 통합 대시보드가 있습니다. 를 AWS CLI 사용하면 특정 정보에 대한 명령을 실행할 수 있습니다.

Viewing Conformance Packs (Console)

에서 적합성 팩을 보려면 적합성 팩 대시보드 팩을 AWS Management Console참조하세요.

Viewing the Details for your Conformance Packs (AWS CLI)

1. 다음 명령을 입력합니다.

```
aws configservice describe-conformance-packs
```

OR

```
aws configservice describe-conformance-packs --conformance-pack-
name="MyConformancePack1"
```

2. 다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
```

```
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "conformancePackInputParameters": [],
    "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"
}
```

Viewing the Status for your Conformance Packs (AWS CLI)

1. 다음 명령을 입력합니다.

```
aws configservice describe-conformance-pack-status --conformance-pack-
name="MyConformancePack1"
```

2. 다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/
awsconfigconforms-MyConformancePack1-conformance-pack-ID/d4301fe0-
a9b1-11e9-994d-025f28dd83ba",
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",
    "conformancePackState": "CREATE_COMPLETE",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
}
```

Viewing the Compliance Status for your Conformance Packs (AWS CLI)

1. 다음 명령을 입력합니다.

```
aws configservice describe-conformance-pack-compliance --conformance-pack-
name="MyConformancePack1"
```

2. 다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackRuleComplianceList": [
```

```
        {
            "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
            "complianceType": "COMPLIANT"
        }
    ]
}
```

Viewing the Compliance Details for your Conformance Packs (AWS CLI)

1. 다음 명령을 입력합니다.

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-
name="MyConformancePack1"
```

2. 다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "conformancePackRuleEvaluationResults": [
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName1-conformance-
pack-ID",
                    "resourceType": "AWS::::Account"
                }
            },
            "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
            "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
```

```
                    "configRuleName": "awsconfigconforms-RuleName2-conformance-
pack-ID",
                    "resourceType": "AWS::EC2::SecurityGroup"
                }
            },
           "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "complianceType": "COMPLIANT"
        }
    ],
    "conformancePackName": "MyConformancePack1"
}
}
```

에 대한 적합성 팩의 규정 준수 기록 타임라인 보기 AWS Config

AWS Config 는 규정 준수 상태 변경 사항을 적합성 팩에 저장할 수 있도록 지원합니다. 이를 통해 규정 준수 상태 변경 이력을 볼 수 있습니다. 이러한 규정 준수 상태 변경은 타임라인으로 표시됩니다. 타임라인은 일정 기간 동안 변경 사항을 `ConfigurationItems`로 캡처합니다. 이 기능을 사용하여 적합성 팩 내에서 규정을 준수하지 않는 특정 규칙을 찾을 수도 있습니다.

AWS Config의 모든 리소스 유형을 기록하도록 수락 또는 거부할 수 있습니다. 모든 리소스 유형을 기록하도록 선택한 경우는 AWS Config 규칙에서 평가한 적합성 팩 규정 준수 기록 기록을 AWS Config 자동으로 시작합니다. 기본적으로는 지원되는 모든 리소스에 대한 구성 변경을 AWS Config 기록합니다. 또한 특정 적합성 팩 규정 준수 이력 리소스 유형만 선택할 수도 있습니다. `AWS::Config::ConformancePackCompliance`. `AWS::Config::ConformancePackCompliance` 리소스 유형 기록은 추가 요금 없이 사용할 수 있습니다. 자세한 내용은 AWS 리소스 기록을 참조하세요.

적합성 팩의 모든 규칙을 준수할 경우 적합성 팩은 규정 준수 상태입니다. 규정을 준수하지 않는 규칙이 하나라도 있으면 규정 미준수 상태입니다. 데이터 부족으로 인해 적합성 팩 내의 모든 규칙을 평가할 수 없는 경우에만 적합성 팩의 규정 준수 상태가 데이터 부족입니다. 적합성 팩의 일부 규칙은 규정 준수 상태이지만 동일한 적합성 팩의 다른 규칙은 데이터 부족인 경우 이 적합성 팩은 규정 준수 상태로 표시됩니다. 적합성 팩의 규정 준수는 한 번에 모두 평가되지 않습니다. 일부 규칙은 다른 규칙보다 평가하는 데 시간이 더 오래 걸릴 수 있습니다. 규정 준수는 규칙 그룹에 대해 한 번에 평가되며, 적합성 팩의 모든 규칙이 평가될 때까지 단계적으로 계속됩니다.

규정 준수 타임라인 보기

적합성 팩 기본 페이지에서 특정 적합성 팩을 선택하여 규정 준수 타임라인에 액세스합니다.

1. 적합성 팩 페이지로 이동합니다.
2. 적합성 팩 기본 페이지에서 특정 적합성 팩을 선택한 다음 적합성 팩 타임라인을 선택합니다.

> **Note**
>
> 또는 적합성 팩의 세부 정보 페이지에서 규정 준수 타임라인을 사용할 수도 있습니다. 적합성 팩을 선택하고 작업 드롭다운에서 세부 정보 보기를 선택합니다. 이 페이지에서 적합성 팩 타임라인을 선택합니다.

타임라인에는 적합성 팩의 규정 준수 상태 변경 이력이 표시됩니다. 다음을 수행할 수 있습니다.

1. 규정 준수 변경 사항을 확장하여 적합성 팩 내 각 규칙의 규정 준수 상태를 한 줄씩 확인할 수 있습니다.
2. 확장된 보기에서 특정 규칙을 선택하여 세부 정보 페이지를 봅니다.

에 대한 적합성 팩의 규정 준수 기록 쿼리 AWS Config

`AWS::Config::ConformancePackCompliance` 리소스 유형을 사용하여 get-resource-config-history를 통해 규정 준수 이력을 쿼리합니다.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "configurationItems": [
        {
            "version": "1.3",
            "accountId": "Account ID",
            "configurationItemCaptureTime": 1614641951.442,
            "configurationItemStatus": "OK",
            "configurationStateId": "1614641951442",
            "configurationItemMD5Hash": "",
```

```
            "arn": "arn:aws:config:us-east-1:Account ID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        },
        {
            "version": "1.3",
            "accountId": "768311917693",
            "configurationItemCaptureTime": 1605551029.515,
            "configurationItemStatus": "ResourceDiscovered",
            "configurationStateId": "1605551029515",
            "configurationItemMD5Hash": "",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
```

```
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        }
    ]
}
```

자세한 내용은 API 참조의 지원되는 리소스 유형(AWS Config) 및 GetResourceConfigHistory를 참조하세요.

조직의 모든 계정에서 AWS Config 에 대한 적합성 팩 관리

AWS Config 를 사용하여 조직 AWS 계정 내 모든에서 적합성 팩을 관리합니다. 다음을 수행할 수 있습니다.

- AWS Organizations의 조직 내 멤버 계정 전체에 적합성 팩을 중앙에서 배포, 업데이트 및 삭제합니다.
- 모든 계정에 공통 규칙 AWS Config 및 문제 해결 작업 세트를 배포하고 AWS Config 규칙 및 문제 해결 작업을 생성해서는 안 되는 계정을 지정합니다.
- 의 관리 계정을 사용하여 조직의 멤버 계정에서 기본 AWS Config 규칙 및 문제 해결 작업을 수정할 수 없도록 하여 거버넌스를 AWS Organizations 적용합니다.

고려 사항

여러 리전에 배포하는 경우

계정 간에 규칙 및 적합성 팩을 배포하기 위한 API 호출은 AWS 리전별로 다릅니다. 규칙을 다른 리전에 배포하려면 조직 수준에서 API 직접 호출의 컨텍스트를 다른 리전으로 변경해야 합니다. 예를 들어 미국 동부(버지니아 북부)에 규칙을 배포하려면 리전을 미국 동부(버지니아 북부)로 변경한 다음 `PutOrganizationConfigRule`을 직접적으로 호출합니다.

조직 내 계정의 경우

새 계정이 조직에 가입하면 규칙 또는 적합성 팩이 해당 계정에 배포됩니다. 계정이 조직을 나가면 규칙 또는 적합성 팩이 제거됩니다.

조직 관리자 계정에 조직 규칙 또는 적합성 팩을 배포한 다음 위임된 관리자를 설정하고 위임된 관리자 계정에 조직 규칙 또는 적합성 팩을 배포하는 경우 위임된 관리자 계정에서 조직 관리자 계정의 조직

규칙 또는 적합성 팩을 볼 수 없고 조직 관리자 계정에서 위임된 관리자 계정의 조직 규칙 또는 적합성 팩을 볼 수 없습니다. DescribeOrganizationConfigRules및 DescribeOrganizationConformancePacks API는 이러한 API를 호출하는 계정에 배포된 조직 관련 리소스만 보고 상호 작용할 수 있습니다.

조직에 추가된 새 계정에 대한 재시도 메커니즘

레코더를 사용할 수 없는 경우 조직에 계정을 추가한 후 7시간 동안만 기존 조직 규칙 및 적합성 팩 배포가 다시 시도됩니다. 조직에 계정을 추가한 후 7시간 이내에 레코더가 없으면 레코더를 생성해야 합니다.

조직 관리 계정, 위임된 관리자 및 서비스 연결 역할

조직 관리 계정을 사용 중이고 조직 배포에 위임된 관리자를 사용하려는 경우 AWS Config 가 서비스 연결 역할(SLR)을 자동으로 생성하지 않는다는 점에 유의하세요. IAM을 사용하여 별도의 서비스 연결 역할(SLR)을 수동으로 생성해야 합니다.

관리 계정에 대한 SLR이 없는 경우 위임된 관리자 계정에서 해당 계정에 리소스를 배포할 수 없습니다. 관리 및 위임된 관리자 계정에서도 멤버 계정에 적합성 팩을 배포할 수 있습니다. 자세한 내용은 AWS Identity and Access Management (IAM) 사용 설명서의 서비스 연결 역할 사용을 참조하세요.

배포

To deploy with the AWS Management Console

AWS 콘솔에서 조직 전체에 적합성 팩을 배포하려면를 사용합니다 AWS Systems Manager. 자세한 내용은 AWS Systems Manager 사용 설명서의 AWS Config 적합성 팩 배포를 참조하세요.

To deploy with the AWS API

AWS Config 와 통합하는 방법에 대한 자세한 내용은 AWS Organizations 사용 설명서의 AWS Config 및 AWS Organizations 섹션을 AWS Organizations참조하세요. 다음 APIs를 사용하여 조직 AWS 계정 내 모든에서 적합성 팩 규칙을 관리하기 전에 AWS Config 기록이 켜져 있는지 확인합니다.

- DeleteOrganizationConformancePack - 해당 조직의 모든 멤버 계정에서 지정된 조직 적합성 팩과 모든 구성 규칙과 문제 해결 작업을 삭제합니다.
- DescribeOrganizationConformancePacks - 조직 적합성 팩의 목록을 반환합니다.
- DescribeOrganizationConformancePackStatuses - 조직의 조직 적합성 팩 배포 상태를 제공합니다.
- GetOrganizationConformancePackDetailedStatus - 특정 조직 적합성 팩에 대한 조직 내 각 멤버 계정의 세부 상태를 반환합니다.

- PutOrganizationConformancePack은 AWS 조직의 멤버 계정에 적합성 팩을 배포합니다.

리전 지원

AWS 조직의 멤버 계정에 적합성 팩을 배포하는 것은 다음 리전에서 지원됩니다.

리전 이름	지역	엔드포인트	프로토콜
미국 동부(오하이오)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
미국 동부(버지니아 북부)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
미국 서부(캘리포니아 북부)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
미국 서부(오레곤)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
아프리카(케이프타운)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
아시아 태평양(홍콩)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
아시아 태평양(하이데라바드)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
아시아 태평양(자카르타)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(멜버른)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
아시아 태평양(뭄바이)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
아시아 태평양(오사카)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
아시아 태평양(서울)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
아시아 태평양(시드니)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
아시아 태평양(도쿄)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
캐나다(중부)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
캐나다 서부(캘거리)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
유럽(프랑크푸르트)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
유럽(아일랜드)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
유럽(런던)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
유럽(밀라노)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
유럽(파리)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
유럽(스페인)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
유럽(스톡홀름)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
유럽(취리히)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
이스라엘(텔아비브)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
중동(바레인)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
중동(UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
남아메리카(상파울루)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
AWS GovCloud(미국 동부)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 서부)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

용 적합성 팩 문제 해결 AWS Config

적합성 팩을 사용할 때 발생할 수 있는 문제를 해결하려면 다음 문제를 확인하세요.

주제

- 적합성 팩의 실패 상태
- 적합성 팩의 누락 규칙

적합성 팩의 실패 상태

적합성 팩을 생성, 업데이트 또는 삭제하는 중에 적합성 팩이 실패했음을 나타내는 오류가 발생하는 경우 적합성 팩의 상태를 확인할 수 있습니다.

```
aws configservice describe-conformance-pack-status --conformance-pack-name
 MyConformancePack1
```

다음과 유사한 출력 화면이 표시되어야 합니다.

```
"ConformancePackStatusDetails": [
    {
        "ConformancePackName": "ConformancePackName",
        "ConformancePackId": "ConformancePackId",
        "ConformancePackArn": "ConformancePackArn",
        "ConformancePackState": "CREATE_FAILED",
        "StackArn": "CloudFormation stackArn",
        "ConformancePackStatusReason": "Failure Reason",
```

```
        "LastUpdateRequestedTime": 1573865201.619,
        "LastUpdateCompletedTime": 1573864244.653
    }
]
```

실패에 대한 자세한 내용은 ConformancePackStatusReason을 확인하세요.

StackArn이 응답에 있는 경우

오류 메시지가 명확하지 않거나 내부 오류로 인한 실패인 경우 AWS CloudFormation 콘솔로 이동하여 다음을 수행합니다.

1. 출력에서 stackArn을 검색합니다.
2. CloudFormation 스택의 이벤트 탭을 선택하고 실패한 이벤트가 있는지 확인합니다.

   상태 이유는 적합성 팩이 실패한 이유를 나타냅니다.

StackArn이 응답에 없는 경우

적합성 팩을 만드는 중에 실패 메시지가 표시되지만 stackArn이 상태 응답에 없는 경우, 가능한 이유는 스택 생성이 실패하고 CloudFormation이 롤백되고 스택이 삭제되었기 때문입니다. CloudFormation 콘솔로 이동하여 삭제됨 상태의 스택을 검색합니다. 실패한 스택을 거기에서 사용할 수 있습니다. CloudFormation 스택에는 적합성 팩 이름이 포함되어 있습니다. 실패한 스택을 찾으면 CloudFormation 스택의 이벤트 탭을 선택하고 실패한 이벤트가 있는지 확인합니다.

이러한 단계로 전혀 해결할 수 없고 실패 원인이 내부 서비스 오류인 경우 작업을 다시 시도하거나 AWS Support 센터에 문의하세요.

적합성 팩의 누락 규칙

적합성 팩을 배포하려면 적합성 팩 템플릿에 규칙을 배포하기 위해 백그라운드에서 기본 AWS CloudFormation 스택을 생성해야 합니다. 이러한 규칙은 서비스 연결 규칙이며 적합성 팩 외부에서 업데이트하거나 삭제할 수 없습니다.

기본 CloudFormation 스택을 변경하면 적합성 팩과 해당 규칙을 관리할 수 없는 상황이 발생합니다. 이러한 관리 불가능한 규칙을 누락 규칙이라고 합니다.

CloudFormation 스택과 적합성 팩 간의 드리프트

CloudFormation 콘솔에서 직접 적합성 팩 템플릿의 규칙 이름을 업데이트할 수 있습니다. CloudFormation 콘솔에서 템플릿을 직접 업데이트해도 배포된 적합성 팩은 업데이트되지 않습니다.

이 드리프트는 누락 규칙을 생성합니다. 적합성 팩에서 규칙을 삭제하려고 하면 다음과 유사한 오류가 발생합니다.

```
"An AWS service owns ServiceLinkedConfigRule. You do not have permissions to
 take action on this rule. (Service: AmazonConfig; Status Code: 400; Error Code:
 AccessDeniedException; Request ID: my-request-ID; Proxy: null)".
```

적합성 팩을 삭제하려고 하면 누락 규칙을 삭제할 수 없으며 다음과 유사한 오류가 발생합니다.

```
"User: arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForConfigConforms/
AwsConfigConformsWorkflow is not authorized to perform: config:DeleteConfigRule on
 resource: my-dangling-rule
```

이 문제를 해결하려면 아래 단계를 따르세요.

1. 스택을 삭제합니다. 자세한 내용은 CloudFormation 사용 설명서의 AWS CloudFormation 콘솔에서 스택 삭제를 참조하세요.
2. AWS Config 콘솔을 사용하거나 DeleteConformancePack API를 사용하여 적합성 팩을 삭제합니다. 조직 적합성 팩이고 관리 또는 위임된 관리자 계정을 사용하는 경우 DeleteOrganizationConformancePack API를 사용합니다.
3. 적합성 팩에 있는 누락 규칙의 Amazon 리소스 이름(ARN)으로 AWS Support 센터에 문의하여 계정을 정리하는 데 도움을 받을 수 있습니다.

이 문제를 방지하려면 다음 모범 사례를 기억하세요.

- 적합성 팩의 CloudFormation 스택을 직접 업데이트하지 마세요.
- 적합성 팩과 기본 CloudFormation 스택 간에 드리프트를 생성하는 변경을 시도하지 마세요.
- 적합성 팩의 서비스 연결 역할(SLR)은 수정할 수 없습니다. 업데이트하려는 리소스가 SLR에 대한 권한 정책의 일부인지 확인합니다.

적합성 팩에 대해 삭제된 CloudFormation 스택

CloudFormation 스택과 적합성 팩 사이에 변동이 없는 한 적합성 팩 또는 해당 CloudFormation 스택의 규칙을 CloudFormation 콘솔에서 직접 삭제하는 것은 권장되지 않습니다.

이 문제를 해결하려면 적합성 팩에 있는 누락 규칙의 Amazon 리소스 이름(ARN)으로 AWS Support 센터에 문의하여 계정을 정리하세요.

이 문제를 방지하려면 다음 모범 사례를 기억하세요.

- 적합성 팩의 기본 CloudFormation 스택을 삭제하지 마세요.
- DeleteConformancePack API를 사용하여 적합성 팩을 삭제합니다. 조직 적합성 팩이고 관리 또는 위임된 관리자 계정을 사용하는 경우 DeleteOrganizationConformancePack API를 사용합니다.

를 사용하여 규정 미준수 리소스 문제 해결 AWS Config

AWS Config 를 사용하면에서 평가한 규정 미준수 리소스를 수정할 수 있습니다 AWS Config 규칙. AWS Config 는 AWS Systems Manager 자동화 문서를 사용하여 문제 해결을 적용합니다. 이러한 문서는에서 평가하는 규정 미준수 AWS 리소스에 대해 수행할 작업을 정의합니다 AWS Config 규칙. AWS Management Console 에서 또는 API를 사용하여 SSM 문서를 연결할 수 있습니다.

AWS Config 는 문제 해결 작업이 포함된 관리형 자동화 문서 세트를 제공합니다. 사용자 지정 자동화 문서를 생성하고 AWS Config 규칙과 연결할 수도 있습니다.

주제

- 리전 지원
- 에 대한 수동 문제 해결 설정 AWS Config
- 에 대한 자동 문제 해결 설정 AWS Config
- 에 대한 수정 작업 삭제 AWS Config

리전 지원

현재 AWS Config 규칙에 대한 수정 작업은 다음 리전에서 지원됩니다.

리전 이름	지역	엔드포인트	프로토콜
미국 동부 (오하이오)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
미국 동부 (버지니아 북부)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
미국 서부 (캘리포니아 북부)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
미국 서부 (오레곤)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아프리카(케이프타운)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
아시아 태평양(홍콩)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
아시아 태평양(하이데라바드)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
아시아 태평양(자카르타)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
아시아 태평양(멜버른)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
아시아 태평양(뭄바이)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
아시아 태평양(오사카)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
아시아 태평양(서울)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(시드니)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
아시아 태평양(도쿄)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
캐나다(중부)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
캐나다 서부(캘거리)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
유럽(프랑크푸르트)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
유럽(아일랜드)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
유럽(런던)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
유럽(밀라노)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
유럽(파리)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
유럽(스페인)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
유럽(스톡홀름)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
유럽(취리히)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
이스라엘(텔아비브)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
중동(바레인)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
중동(UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
남아메리카(상파울루)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 동부)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 서부)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

에 대한 수동 문제 해결 설정 AWS Config

규정을 준수하지 않는 리소스에 문제 해결을 적용하려면 미리 채워진 목록에서 연결할 문제 해결 작업을 선택하거나 SSM 문서를 사용하여 사용자 지정 문제 해결 작업을 생성할 수 있습니다.는에서 권장 문제 해결 작업 목록을 AWS Config 제공합니다 AWS Management Console.

Setting Up Manual Remediation (Console)

에서 문제 해결 작업을 AWS Config 규칙과 연결하여 규정 미준수 리소스를 수동으로 해결하도록 선택할 AWS Management Console수 있습니다. 모든 문제 해결 작업에서 수동 또는 자동 문제 해결을 선택할 수 있습니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 왼쪽에서 규칙을 선택한 후 규칙 페이지에서 규칙 추가를 선택하여 규칙 목록에 새 규칙을 추가합니다.

   기존 규칙의 경우 규칙 목록에서 규정 미준수 규칙을 선택하고 작업 드롭다운 목록을 선택합니다.
3. 작업 드롭다운 목록에서 문제 해결 관리를 선택합니다. '수동 문제 해결'을 선택한 다음 권장 목록에서 적절한 문제 해결 작업을 선택합니다.

   > **Note**
   >
   > 서비스 연결되지 않은 AWS Config 규칙에 대한 문제 해결만 관리할 수 있습니다. 자세한 내용은 서비스 연결 AWS 역할을 참조하세요.

   선택한 문제 해결 작업에 따라 특정 파라미터가 나타나거나 파라미터가 전혀 나타나지 않습니다.
4. (선택 사항): 규정 미준수 리소스의 리소스 ID를 문제 해결 작업에 전달하려면 Resource ID parameter(리소스 ID 파라미터)를 선택합니다. 이 항목을 선택하면 실행 시간에 해당 파라미터는 문제 해결할 리소스의 ID로 대체됩니다.

   각 파라미터에는 정적 값 또는 동적 값이 있습니다. 드롭다운 목록에서 특정 리소스 ID 파라미터를 선택하지 않은 경우 각 키의 값을 입력할 수 있습니다. 드롭다운 목록에서 특정 리소스 ID 파라미터를 선택한 경우 선택한 리소스 ID 파라미터를 제외하고 기타 모든 키의 값을 입력할 수 있습니다.
5. 저장을 선택합니다. Rules(규칙) 페이지가 표시됩니다.

실패한 문제 해결 작업의 경우 AWS 명령줄 인터페이스 명령을 실행`describe-remediation-execution-status`하여 리소스 세트에 대한 문제 해결 실행을 자세히 볼 수 있습니다. 세부 정보에는 상태, 수정 실행 단계의 타임스탬프 및 실패한 단계에 대한 오류 메시지가 포함됩니다.

Setting Up Manual Remediation (API)

다음 AWS Config API 작업을 사용하여 수동 문제 해결을 설정합니다.

- PutRemediationConfigurations는 선택한 대상 또는 작업이 있는 특정 AWS Config 규칙으로 문제 해결 구성을 추가하거나 업데이트합니다.
- StartRemediationExecution은 마지막으로 알려진 문제 해결 구성에 대해 지정된 AWS Config 규칙에 대한 온디맨드 문제 해결을 실행합니다.
- DescribeRemediationExecutionStatus, 실패한 단계의 상태, 문제 해결 실행 단계가 발생한 타임스탬프 및 오류 메시지를 포함하여 리소스 집합에 대한 해결 작업 실행에 대한 상세 보기를 제공합니다.
- DescribeRemediationConfigurations, 하나 이상의 해결 작업 구성에 대한 세부 정보를 반환합니다.

에 대한 자동 문제 해결 설정 AWS Config

규정 미준수 리소스에 문제 해결을 적용하려면 미리 채워진 목록에서 연결할 문제 해결 작업을 선택하거나 SSM 문서를 사용하여 사용자 지정 문제 해결 작업을 생성할 수 있습니다.는에 문제 해결 작업 목록을 AWS Config 제공합니다 AWS Management Console.

Setting Up Auto Remediation (Console)

에서 문제 해결 작업을 AWS Config 규칙과 연결하여 규정 미준수 리소스를 자동으로 해결하도록 선택할 AWS Management Console수 있습니다. 모든 문제 해결 작업에서 수동 또는 자동 문제 해결을 선택할 수 있습니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 왼쪽에서 규칙을 선택한 후 규칙 페이지에서 규칙 추가를 선택하여 규칙 목록에 새 규칙을 추가합니다.

   기존 규칙의 경우 규칙 목록에서 규정 미준수 규칙을 선택하고 작업 드롭다운 목록을 선택합니다.
3. 작업 드롭다운 목록에서 문제 해결 관리를 선택합니다. "자동 문제 해결"을 선택한 다음 목록에서 적절한 문제 해결 작업을 선택합니다.

> **Note**
>
> 서비스 연결되지 않은 AWS Config 규칙에 대한 문제 해결만 관리할 수 있습니다. 자세한 내용은 서비스 연결 AWS 역할을 참조하세요.

선택한 문제 해결 작업에 따라 특정 파라미터가 나타나거나 파라미터가 전혀 나타나지 않습니다.

4. 규정 미준수 리소스 문제를 자동으로 해결하려면 자동 문제 해결을 선택합니다.

   자동 문제 해결 후에도 리소스가 계속 규정을 준수하지 않는 경우, 자동 문제 해결을 다시 시도하도록 규칙을 설정할 수 있습니다. 원하는 재시도 횟수와 시간(초)을 입력합니다.

   > **Note**
   >
   > 문제 해결 스크립트를 여러 번 실행하면 비용이 발생합니다. 재시도는 문제 해결이 실패하고 지정된 기간 내에 작동하는 경우에만 발생합니다(예: 300초 내에 5회 재시도). 자세한 내용은 Systems Manager Automation 요금을 참조하세요.

5. (선택 사항): 규정 미준수 리소스의 리소스 ID를 문제 해결 작업에 전달하려면 Resource ID parameter(리소스 ID 파라미터)를 선택합니다. 이 항목을 선택하면 실행 시간에 해당 파라미터는 문제 해결할 리소스의 ID로 대체됩니다.

   각 파라미터에는 정적 값 또는 동적 값이 있습니다. 드롭다운 목록에서 특정 리소스 ID 파라미터를 선택하지 않은 경우 각 키의 값을 입력할 수 있습니다. 드롭다운 목록에서 특정 리소스 ID 파라미터를 선택한 경우 선택한 리소스 ID 파라미터를 제외하고 기타 모든 키의 값을 입력할 수 있습니다.

6. 저장을 선택합니다. Rules(규칙) 페이지가 표시됩니다.

실패한 해결 작업 문제 해결

실패한 문제 해결 작업의 경우 AWS 명령줄 인터페이스 명령을 실행`describe-remediation-execution-status`하여 리소스 세트에 대한 문제 해결 실행을 자세히 볼 수 있습니다. 세부 정보에는 상태, 수정 실행 단계의 타임스탬프 및 실패한 단계에 대한 오류 메시지가 포함됩니다.

규정을 준수하는 리소스에 대한 자동 해결 작업 실행

PutRemediationConfigurations API 또는 AWS Config 콘솔을 사용하여 특정 AWS Config 규칙에 대한 자동 문제 해결을 활성화하면 해당 특정 규칙에 대한 모든 규정 미준수 리소스에 대한 문제 해결 프로세스가 시작됩니다. 자동 해결 작업 프로세스는 정기적으로 캡처되는 규정 준수 데이터 스냅샷에 의존합니다. 스냅샷 일정 사이에 업데이트된 모든 규정 미준수 리소스는 마지막으로 알려진 규정 준수 데이터 스냅샷을 기반으로 계속 수정됩니다.

즉, 부트스트랩 프로세서는 마지막으로 알려진 규정 준수 데이터 스냅샷을 기반으로 오래된 평가 결과를 가질 수 있는 데이터베이스를 사용하기 때문에 규정 준수 리소스에 대해서도 자동 해결 작업을 시작할 수 있습니다.

Setting Up Auto Remediation (API)

다음 AWS Config API 작업을 사용하여 자동 문제 해결을 설정합니다.

- PutRemediationExceptions는 특정 AWS Config 규칙에 따라 특정 리소스에 대한 새 예외를 추가하거나 기존 예외를 업데이트합니다.
- DescribeRemediationExceptions, 하나 이상의 해결 작업 예외에 대한 세부 정보를 반환합니다.

에 대한 수정 작업 삭제 AWS Config

AWS Config 콘솔 또는를 사용하여 문제 해결 작업을 AWS CLI 삭제할 수 있습니다.

Deleting remediation actions (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 왼쪽에서 규칙을 선택한 후 규칙 페이지의 규칙 목록에서 규칙을 선택한 다음 세부 정보 보기를 선택합니다.
3. ## ## 페이지에서 문제 해결 작업 섹션으로 이동합니다. 섹션을 확장하면 추가 세부 정보를 볼 수 있습니다.
4. 문제 해결 작업 섹션에서 삭제를 선택하고 삭제 작업을 확인합니다.

> **Note**
>
> 진행 중인 문제 해결 작업은 삭제되지 않습니다. 문제 해결 작업 삭제를 선택하면 해당 문제 해결 작업을 검색할 수 없습니다. 문제 해결 작업 삭제는 연결된 규칙을 삭제하지 않습니다.

문제 해결 작업을 삭제하면 리소스 ID 파라미터가 비어 있고 해당 없음으로 표시됩니다. 규칙 페이지의 문제 해결 작업 열에는 관련 규칙에 대해 설정되지 않음이 표시됩니다.

Deleting remediation actions (API)

다음 AWS Config API 작업을 사용하여 자동 문제 해결을 설정합니다.

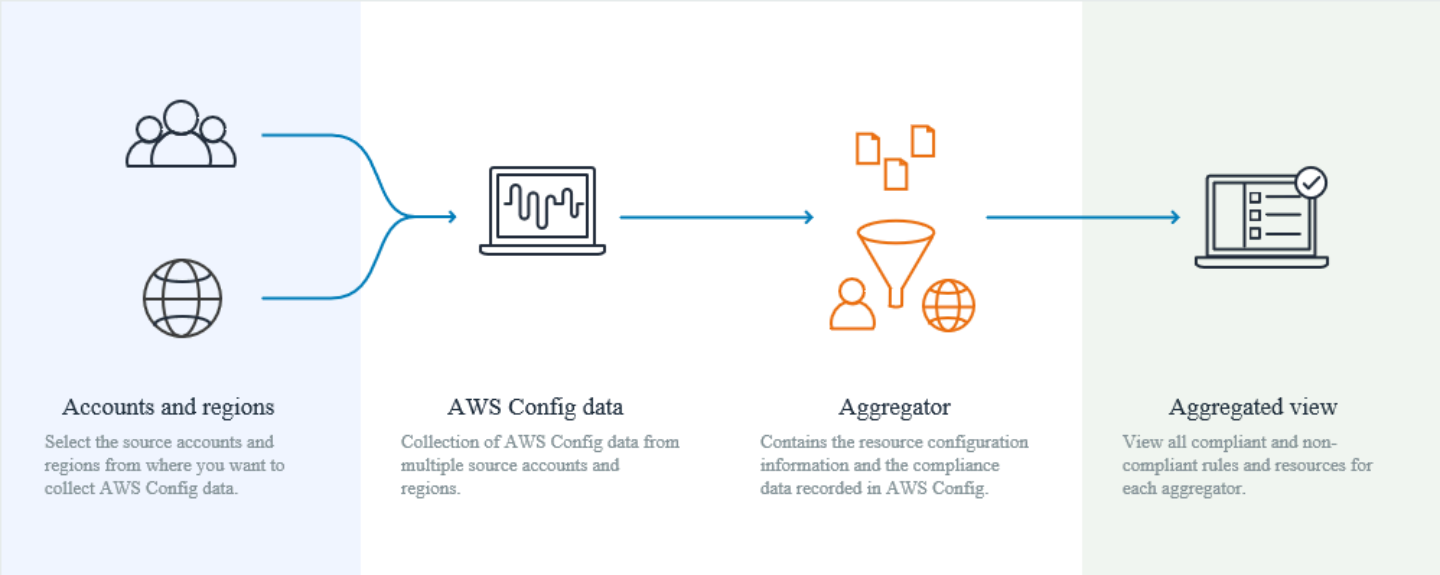
- DeleteRemediationConfiguration, 해결 작업 구성을 삭제합니다.
- DeleteRemediationExceptions, 리소스 키에 언급된 하나 이상의 해결 작업 예외를 삭제합니다.

에 대한 다중 계정 다중 리전 데이터 집계 AWS Config

애그리게이터는 다음에서 AWS Config 구성 및 규정 준수 데이터를 수집하는 AWS Config 리소스 유형입니다.

- 여러 계정 및 여러 AWS 리전.
- 단일 계정 및 여러 AWS 리전.
- 의 조직 AWS Organizations 과가 AWS Config 활성화한 해당 조직의 모든 계정.

집계자를 사용하여 AWS Config에 기록된 리소스 구성 및 규정 준수 데이터를 봅니다. 다음 이미지는 집계자가 여러 계정 및 리전에서 AWS Config 데이터를 수집하는 방법을 보여줍니다.



사용 사례

- 규정 준수 모니터링: 규정 준수 데이터를 집계하여 조직의 전체 규정 준수 태세 또는 계정 및 리전 간 규정 준수 태세를 평가할 수 있습니다.
- 변경 추적: 조직 전체 또는 계정 및 리전 간에 시간 경과에 따른 리소스 변경 사항을 추적할 수 있습니다.
- 리소스 관계: 조직 전체 또는 계정 및 리전 전체의 리소스 종속 항목 및 관계를 분석할 수 있습니다.

> **Note**
>
> 애그리게이터는 소스 계정의 데이터를 애그리게이터 계정으로 복제하여 애그리게이터가 볼 권한을 부여받은 소스 계정 및 리전에 대한 읽기 전용 보기를 제공합니다. 애그리게이터는 소스 계정 또는 리전에 대한 변형 액세스 권한을 제공하지 않습니다. 예를 들어, 애그리게이터를 통해 규칙을 배포하거나, 애그리게이터를 통해 소스 계정 또는 리전으로 스냅샷 파일을 보낼 수 없습니다.
> 애그리게이터를 사용해도 추가 비용이 발생하지 않습니다.

용어

소스 계정은 AWS Config 리소스 구성 및 규정 준수 데이터를 집계하려는 AWS 계정 입니다. 소스 계정은 개별 계정일 수도 있고 AWS Organizations내 조직일 수도 있습니다. 소스 계정을 개별적으로 제공하거나 검색할 수 있습니다 AWS Organizations.

소스 리전은 AWS Config 구성 및 규정 준수 데이터를 집계하려는 AWS 리전입니다.

애그리게이터 계정은 사용자가 애그리게이터를 생성하는 계정입니다.

권한 부여는 AWS Config 구성 및 규정 준수 데이터를 수집하기 위해 애그리게이터 계정 및 리전에 부여하는 권한을 말합니다. AWS Organizations를 구성하는 소스 계정을 집계하는 경우에는 권한 부여가 필요하지 않습니다.

서비스 연결 애그리게이터는 특정 에 연결됩니다 AWS 서비스. 범위 내 구성 및 규정 준수 데이터는 연결된 서비스에 의해 설정됩니다.

리전 지원

현재 다중 계정 다중 리전 데이터 집계는 다음 리전에서 지원됩니다.

리전 이름	지역	엔드포인트	프로토콜	
미국 동부 (오하이오)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	

리전 이름	지역	엔드포인트	프로토콜
미국 동부(버지니아 북부)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
미국 서부(캘리포니아 북부)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
미국 서부(오레곤)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
아프리카(케이프타운)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
아시아 태평양(홍콩)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
아시아 태평양(하이데라바드)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
아시아 태평양(자카르타)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
아시아 태평양(말레이시아)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
아시아 태평양(멜버른)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(뭄바이)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
아시아 태평양(오사카)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
아시아 태평양(서울)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
아시아 태평양(시드니)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
아시아 태평양(타이베이)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
아시아 태평양(태국)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
아시아 태평양(도쿄)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
캐나다(중부)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
캐나다 서부(캘거리)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
유럽(프랑크푸르트)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
유럽(아일랜드)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
유럽(런던)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
유럽(밀라노)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
유럽(파리)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
유럽(스페인)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
유럽(스톡홀름)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
유럽(취리히)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
이스라엘(텔아비브)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
멕시코(중부)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
중동(바레인)	me-south-1	config.me-south-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
중동 (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
남아메리카(상파울루)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 동부)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 서부)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

에 대한 집계자 대시보드에서 규정 준수 및 인벤토리 데이터 보기 AWS Config

집계자 페이지의 대시보드에는 집계된 AWS 리소스의 구성 데이터가 표시됩니다. 여기에서는 규칙, 규정 준수 팩 및 규정 준수 상태에 대한 개요를 제공합니다.

대시보드는 총 리소스 수를 제공합니다 AWS . 리소스 유형과 소스 계정은 가장 많은 수의 리소스별로 순위가 매겨집니다. 또한 준수 규칙 및 미준수 규칙의 수가 제공됩니다. 미준수 규칙은 가장 많은 수의 미준수 리소스를 기준으로 순위가 매겨집니다. 미준수 규정 준수 팩과 소스 계정은 가장 많은 수의 미준수 규칙을 기준으로 순위가 매겨집니다.

설정 후 지정된 소스 계정의 데이터를 집계자로 집계하기 AWS Config시작합니다. 규칙의 준수 상태가 표시될 때까지 몇 분 정도 걸릴 수 있습니다.

애그리게이터 대시보드 사용

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.

2. 애그리게이터 페이지로 이동합니다. 해당 페이지에서는 다음과 같은 내용을 볼 수 있습니다.

   - 규칙 및 규정 준수 상태.
   - 규정 준수 팩 및 규정 준수 상태.
   - AWS 리소스 및 해당 구성 데이터.
3. 대시보드에서 애그리게이터를 선택합니다. 애그리게이터 이름을 기준으로 애그리게이터를 필터링합니다. 다음과 같은 위젯을 볼 수 있습니다.

   - 리소스 인벤토리

     선택한 애그리게이터의 상위 10개 리소스 유형을 리소스 수에 따라 내림차순으로 볼 수 있습니다. 리소스 인벤토리 뒤의 괄호 안에 표시되는 선택한 애그리게이터의 총 리소스 수를 선택하면 애그리게이터의 모든 리소스를 볼 수 있는 집계된 리소스 페이지로 이동할 수 있습니다. 또는 위젯에서 리소스 유형을 선택하면 리소스 유형을 사용하여 필터링되는 집계된 리소스 페이지로 이동합니다.
   - 리소스 개수별 계정

     선택한 애그리게이터의 상위 5개 계정 유형을 리소스 수에 따라 내림차순으로 볼 수 있습니다. 위젯에서 계정을 선택하면 지정된 계정을 사용하여 필터링되는 리소스 페이지로 이동합니다.
   - 미준수 규칙

     선택한 집계자의 상위 5개 규정 미준수 규칙을 규정 미준수 리소스 수를 기준으로 내림차순으로 확인합니다. 위젯에서 규칙을 선택하면 지정된 규칙의 세부 정보 페이지로 이동합니다. 전체 미준수 규칙 보기를 선택하면 애그리게이터에 대한 모든 규칙을 볼 수 있는 집계된 규칙 페이지로 이동합니다.
   - 미준수 규칙별 계정

     선택한 애그리게이터의 상위 5개 계정을 미준수 규칙 수에 따라 내림차순으로 볼 수 있습니다. 위젯에서 계정을 선택하면 지정된 계정을 사용하여 필터링된 애그리게이터에 대한 모든 규칙을 볼 수 있는 집계된 규칙 페이지로 이동합니다.
   - 미준수 규정 준수 팩별 계정

     선택한 애그리게이터의 상위 5개 계정을 미준수 규정 준수 팩 수에 따라 내림차순으로 볼 수 있습니다. 위젯에서 계정을 선택하면 지정된 계정을 사용하여 필터링된 애그리게이터에 대한 모든 규정 준수 팩을 볼 수 있는 집계된 규정 준수 팩 페이지로 이동합니다.
4. 왼쪽 탐색 창의 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.

   - 규정 준수 대시보드

애그리게이터 내에서 리소스 규정 준수에 대한 인사이트를 요약하는 위젯을 사용하여 자동화된 규정 준수 대시보드를 확인합니다. 미준수 리소스별 상위 10개 리소스 유형, 미준수 규칙별 상위 10개 계정 수준 준수 팩 등의 데이터를 볼 수 있습니다. 이러한 그래프와 차트에 대한 자세한 내용은 규정 준수 대시보드를 참조하세요.

- 적합성 팩

  집계자 AWS 계정 내에서 생성되고 다른에 연결된 모든 적합성 팩을 봅니다. 규정 준수 팩 페이지에는 각 규정 준수 팩의 이름, 리전, 계정 ID, 규정 준수 상태를 나열하는 표가 표시됩니다. 이 페이지에서 규정 준수 팩을 선택할 수 있으며, 세부 정보 보기를 통해 규정 준수 팩의 규칙과 리소스, 규정 준수 상태에 대한 자세한 내용을 볼 수 있습니다.

- 규칙

  생성 후 애그리게이터 내의 여러 다른 AWS 계정에 연결된 모든 규칙을 확인합니다. 규칙 페이지에는 각 규칙의 이름, 규정 준수 상태, 리전, 계정을 나열하는 표가 표시됩니다. 이 페이지에서 규칙을 선택할 수 있으며, 세부 정보 보기를 통해 애그리게이터, 리전, 계정 ID, 범위 내 리소스 등에 대한 내용을 볼 수 있습니다.

- 인벤토리 대시보드

  애그리게이터 내에서 리소스 구성 데이터에 대한 인사이트를 요약하는 위젯을 사용하여 자동화된 인벤토리 대시보드를 확인합니다. 리소스 개수별 상위 10개 리소스 유형, 리소스 개수별 상위 10개 계정 등의 데이터를 볼 수 있습니다. 이러한 그래프와 차트에 대한 자세한 내용은 인벤토리 대시보드를 참조하세요.

- 리소스

  기록된 후 애그리게이터 내의 여러 다른 AWS 계정에 연결된 모든 리소스를 확인합니다. 리소스 페이지에서 리소스를 선택할 수 있으며, 세부 정보 보기를 통해 리소스의 세부 정보, 관련 규칙, 현재 리소스 구성을 볼 수 있습니다. 리소스의 애그리게이터, 리전, 계정 ID, 리소스 이름, 리소스 유형, 리소스 ID 등과 같은 리소스에 대한 정보도 볼 수 있습니다.

- 권한 부여

  현재 권한이 부여되었거나 권한 부여 대기 중인 모든 계정을 보고 관리할 수 있습니다. 권한 부여 페이지에서 권한 추가를 선택하면 다른 계정에 대한 액세스 권한을 제공할 수 있습니다. 계정 ID에서 액세스 권한을 취소하려면 권한 삭제를 선택합니다.

> **Note**
>
> 문제 해결
>
> 다음과 같은 이유로 모든 소스 계정 및 리전의 데이터 컬렉션이 집계된 보기에 불완전한 메시지가 표시될 수 있습니다.
>
> - AWS 리소스의 규정 미준수 AWS Config 규칙 및 구성 데이터 전송이 진행 중입니다.
> - AWS Config 에서 적용한 필터와 일치하는 규칙을 찾을 수 없습니다. 적절한 계정 또는 리전을 선택하고 다시 시도하세요.
>
> 집계된 보기에 조직의 데이터 수집이 불완전하다는 메시지가 표시될 수 있습니다. You can view the below data only for 24 hours(조직의 데이터 수집이 완전하지 않습니다. 24시간 동안의 데이터만 아래에서 볼 수 있습니다). 이 메시지가 표시되는 이유는 다음과 같습니다.
>
> - AWS Config 는 유효하지 않은 IAM 역할로 인해 조직 세부 정보에 액세스할 수 없습니다. IAM 역할이 24시간 이상 유효하지 않은 상태로 있을 경우, AWS Config 가 전체 조직의 데이터를 삭제합니다.
> - AWS Config 조직에서 서비스 액세스가 비활성화되었습니다.

규정 준수 대시보드

애그리게이터 내에서 리소스 규정 준수에 대한 인사이트를 요약하는 위젯을 사용하여 자동화된 규정 준수 대시보드를 확인합니다. 이 대시보드는 규정 준수 결과가 있는 규칙만 표시합니다.

> **Note**
>
> 제한 사항
>
> 규정 준수 대시보드의 인사이트는의 고급 쿼리 기능에서 제공하며 AWS Config,이 기능은 중첩 구조 또는 중첩 배열 언패킹을 지원하지 않습니다. 즉, 규정 준수 대시보드에는 리소스에 대해 보고하는 각 특정 규칙의 규정 준수 상태가 아니라 리소스의 전체 규정 준수가 표시됩니다. 예를 들어 리소스 유형 `AWS::Config::ResourceCompliance`에 대한 구성 항목(CI)을 확인하는 경우 대시보드는 해당 리소스에 대해 보고하는 모든 규칙에 대한 규정 준수 결과를 표시합니다. 리소스에 대해 보고하는 규칙이 10개 있고 이 중 9개는 COMPLIANT이고 1개만 NON_COMPLIANT인 경우 해당 리소스의 전체 규정 준수는 NON_COMPLIANT입니다.

리소스별 규정 준수 요약

선택한 애그리게이터의 규정 미준수 리소스 수와 규정 준수 리소스 수를 비교하는 파이 차트가 표시됩니다. 차트 위에 마우스 커서를 올리면 규정 준수 리소스 및 규정 미준수 리소스의 정확한 개수와 비율을 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다.

규정 미준수 리소스별 상위 10개 리소스 유형

선택한 애그리게이터의 리소스 유형 10개를 규정 미준수 리소스 개수별로 내림차순으로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스 커서를 올리면 각 리소스 유형에 대한 규정 미준수 리소스의 정확한 개수를 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다.

규정 미준수 리소스별 상위 10개 계정

규정 미준수 리소스별 상위 10개 계정에는 선택한 애그리게이터의 계정 10개를 규정 미준수 리소스 개수별로 내림차순으로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스 커서를 올리면 각 계정에 대한 규정 미준수 리소스의 정확한 개수를 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다.

규정 미준수 리소스별 상위 10개 리전

선택한 애그리게이터가 데이터를 수집하는 리전 10개를 규정 미준수 리소스 개수별로 내림차순으로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스 커서를 올리면 각 리전에 대한 규정 미준수 리소스의 정확한 개수를 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정에 따라 다릅니다.

규정 미준수 규칙별 상위 10개 계정 수준 적합성 팩

선택한 애그리게이터의 계정 수준 적합성 팩 10개를 규정 미준수 규칙 개수별로 내림차순으로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스 커서를 올리면 각 계정 수준 적합성 팩에 대한 규정 준수 규칙 및 규정 미준수 규칙의 비율을 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다.

규정 미준수 규칙별 상위 10개 조직 수준 적합성 팩

선택한 애그리게이터의 조직 수준 적합성 팩 10개를 규정 미준수 규칙 개수별로 내림차순으로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스 커서를 올리면 각 조직 수준 적합성 팩에 대한 규정 준수 규칙 및 규정 미준수 규칙의 비율을 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다.

적합성 팩 전체의 규정 미준수 규칙별 상위 10개 계정

적합성 팩 전체의 규정 미준수 리소스별 상위 10개 계정에는 선택한 애그리게이터의 계정 10개를 모든 적합성 팩 전체의 규정 미준수 규칙 개수별로 내림차순으로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스 커서를 올리면 각 계정에 대한 규정 미준수 규칙의 정확한 개수를 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다.

인벤토리 대시보드

애그리게이터 내에서 리소스 구성 데이터에 대한 인사이트를 요약하는 위젯을 사용하여 자동화된 인벤토리 대시보드를 확인합니다.

리소스 개수별 상위 10개 리소스 유형

선택한 애그리게이터의 리소스 유형 10개를 리소스 개수별로 내림차순으로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스를 올려놓으면 각 리소스 유형에 대한 규정 미준수 리소스의 정확한 개수를 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다.

리전별 리소스 수

선택한 애그리게이터가 데이터를 수집하는 리전 10개를 리소스 개수별로 내림차순으로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스를 올려놓으면 각 리전의 정확한 개수를 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정에 따라 다릅니다.

리소스 개수별 상위 10개 계정

선택한 애그리게이터의 계정 10개를 리소스 개수별로 내림차순으로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스를 올려놓으면 각 리소스 유형에 대한 규정 미준수 리소스의 정확한 개수를 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다.

Amazon EC2 서비스 리소스 유형별 리소스 수

선택한 애그리게이터의 Amazon EC2 리소스 유형을 리소스 개수별로 내림차순으로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스를 올려놓으면 각 Amazon EC2 리소스 유형에 대한 규정 미준수 리소스의 정확한 개수를 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다. 이 차트를 사용하려면 Amazon EC2 리소스 유형을 기록하도록 레코더를 구성해야 합니다. 자세한 내용은 AWS Config 기록할 리소스 선택을 참조하세요.

사용된 상위 10개 EC2 인스턴스 유형

선택한 애그리게이터의 Amazon EC2 인스턴스 리소스 유형 10개를 사용량별로 내림차순으로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스를 올려놓으면 각 EC2 인스턴스 유형의 사용량을 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다. 이 차트를 사용하려면 EC2 인스턴스 리소스 유형을 기록하도록 레코더를 구성해야 합니다. 자세한 내용은 AWS 리소스 재코딩을 참조하세요.

볼륨 유형 및 크기별 EBS 볼륨 수

선택한 애그리게이터의 EBS 볼륨을 리소스 개수별로 비교한 세로 막대그래프가 표시됩니다. 그래프 위에 마우스를 올려놓으면 각 EBS 볼륨 유형의 개수 및 크기 분석을 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다. 이 차트를 사용하려면 EC2 볼륨 리소스 유형을 기록하도록 레코더를 구성해야 합니다. 자세한 내용은 AWS Config 기록할 리소스 선택을 참조하세요.

유형별로 실행 중인 EC2 인스턴스와 중지된 EC2 인스턴스 수

선택한 애그리게이터의 실행 중인 EC2 인스턴스 유형과 중지된 EC2 인스턴스를 인스턴스 유형별로 비교하는 가로 막대그래프가 표시됩니다. 그래프 위에 마우스를 올려놓으면 각 유형별로 중지 및 실행 중인 EC2 인스턴스의 정확한 개수를 볼 수 있습니다.

표시되는 데이터는 선택한 애그리게이터의 각 계정에 대한 구성 레코더 설정, 그리고 선택한 애그리게이터가 데이터를 수집하도록 구성된 리전에 따라 다릅니다. 이 차트를 사용하려면 EC2 인스턴스 리소스 유형을 기록하도록 레코더를 구성해야 합니다. 자세한 내용은 AWS 리소스 재코딩을 참조하세요.

에 대한 집계자 생성 AWS Config

AWS Config 콘솔 또는를 사용하여 집계자를 AWS CLI 생성할 수 있습니다. 에서 개별 계정 IDs 추가 또는 데이터를 집계하려는 조직 추가를 선택할 AWS Config 수 있습니다. 의 경우 두 AWS CLI 가지 절차가 있습니다.

Creating Aggregators (Console)

애그리게이터 페이지에서 데이터를 집계할 소스 계정 ID 또는 조직 및 리전을 지정하여 애그리게이터를 생성합니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 집계자 페이지로 이동하여 집계자 생성을 선택합니다.
3. 데이터 복제 허용은 AWS Config 에게 소스 계정에서 집계자 계정으로 데이터를 복제할 권한을 부여합니다.

   소스 계정(들)의 데이터를 집계자 계정으로 복제 AWS Config 하려면 허용을 선택합니다. 집계자를 계속해서 추가하려면 이 확인란을 선택해야 합니다를 선택합니다.
4. 집계자 이름에 집계자의 이름을 입력합니다.

   집계자 이름은 최대 64자의 영숫자로 구성된 고유한 이름이어야 합니다. 이름은 하이픈 및 밑줄을 포함할 수 있습니다.
5. 소스 계정 선택에서 데이터를 집계할 소스로 개별 계정 ID 추가 또는 내 조직 추가를 선택합니다.

> **Note**
> 개별 계정 ID 추가를 사용하여 소스 계정을 선택할 때는 권한 부여가 필요합니다.

- 개별 계정 ID 추가를 선택할 경우, 집계자 계정으로 개별 계정 ID를 추가할 수 있습니다.
  1. 소스 계정 추가를 선택하여 계정 ID를 추가합니다.
  2. Add AWS 계정 IDs를 선택하여 쉼표로 구분된 AWS 계정 IDs 수동으로 추가합니다. 현재 계정으로부터 데이터를 집계하려면 계정의 계정 ID를 입력합니다.

     OR

     파일 업로드를 선택하여 쉼표로 구분된 AWS 계정 ID의 파일(.txt 또는 .csv)을 업로드합니다.
  3. 소스 계정 추가를 선택하여 선택 사항을 확인합니다.
- 내 조직 추가를 선택할 경우. 조직의 모든 계정을 집계자 계정에 추가할 수 있습니다.

> **Note**
> 사용자는 관리 계정이나 등록된 위임된 관리자에 로그인되어 있어야 하고 조직에서 모든 기능이 활성화되어 있어야 합니다. 호출자가 관리 계정인 경우 `EnableAwsServiceAccess` API를 AWS Config 호출하여 AWS Config 와 간의 통합을 활성화합니다 AWS Organizations. 호출자가 등록된 위임된 관리자인 경우 `ListDelegatedAdministrators` API를 AWS Config 호출하여 호출자가 유효한 위임된 관리자인지 확인합니다.
> 위임된 관리자가 집계자를 생성하기 전에 관리 계정이 AWS Config 서비스 보안 주체 이름(config.amazonaws.com)에 위임된 관리자를 등록해야 합니다. 위임된 관리자를 등록하려면 에 위임된 관리자 등록 AWS Config 문서를 참조하세요.

가 조직의 읽기 전용 APIs를 호출할 수 AWS Config 있도록 IAM 역할을 할당해야 합니다.

1. 사용자 계정에서 역할 선택을 선택하여 기존 IAM 역할을 선택합니다.

> **Note**
>
> IAM 콘솔에서 `AWSConfigRoleForOrganizations` 관리형 정책을 IAM 역할에 연결합니다. 이 정책을 연결하면가 `DescribeOrganization`, `ListAWSServiceAccessForOrganization`및 `ListAccounts` API를 호출 AWS Config AWS Organizations 할 수 있습니다. APIs 기본적으로 `config.amazonaws.com`이 신뢰할 수 있는 엔터티로 자동 지정됩니다.

2. 또는 역할 생성을 선택하고 IAM 역할 이름의 이름을 입력하여 IAM 역할을 생성합니다.

6. 리전에서 데이터를 집계하려는 리전을 선택합니다.
   - AWS 리전를 하나, 여러 개 또는 모두 선택합니다.
   - AWS 리전 다중 계정 다중 리전 데이터 집계가 활성화된 모든 미래의 데이터를 집계하려면 미래 포함 AWS 리전을 선택합니다.
7. 저장을 선택합니다. 집계자를 AWS Config 표시합니다.

Creating Aggregators using Individual Accounts (AWS CLI)

1. 명령 프롬프트 또는 터미널 창을 엽니다.
2. 다음 명령을 입력하여 **`MyAggregator`**라는 애그리게이터를 생성합니다.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

   `account-aggregation-sources`에 대해 다음 중 하나를 입력합니다.

   - 데이터를 집계하려는 쉼표로 구분된 AWS 계정 IDs. 계정 ID를 대괄호로 묶고 반드시 따옴표를 이스케이프 처리해야 합니다(예: `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`).
   - 쉼표로 구분된 AWS 계정 계정 ID의 JSON 파일을 업로드할 수도 있습니다. 다음 구문을 사용하여 파일을 업로드합니다. `--account-aggregation-sources MyFilePath/MyFile.json`

     JSON 파일은 다음 형식이어야 합니다.

```
[
    {
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ],
        "AllAwsRegions": true
    }
]
```

3. 입력을 눌러 명령을 실행합니다.

   다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

Creating Aggregators using AWS Organizations (AWS CLI)

이 절차를 시작하기 전에 사용자는 관리 계정 또는 등록된 위임된 관리자로 로그인되어 있어야 하고 조직에서 모든 기능이 활성화되어 있어야 합니다.

> **Note**
>
> 위임된 관리자가 집계자를 생성하기 전에 관리 계정이 다음 AWS Config 서비스 보안 주체 이름(`config.amazonaws.com` 및`config-multiaccountsetup.amazonaws.com`)을 모두 사용하여 위임된 관리자를 등록해야 합니다. 위임된 관리자를 등록하려면 에 위임된 관리자 등록 AWS Config 문서를 참조하세요.

1. 명령 프롬프트 또는 터미널 창을 엽니다.
2. 가 AWS Config 애그리게이터에 대한 IAM 역할을 생성하지 않은 경우 다음 명령을 입력합니다.

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect\":\"Allow\",
\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action\":\"sts:AssumeRole
\"}]}" --description "Role for organizational AWS Config aggregator"
```

> **Note**
>
> 애그리게이터를 생성할 때 사용할이 IAM 역할에서 Amazon 리소스 이름(ARN) AWS Config 을 복사합니다. 응답 객체에서 ARN을 확인할 수 있습니다.

3. IAM 역할에 정책을 연결하지 않은 경우 AWSConfigRoleForOrganizations 관리형 정책을 연결하거나 다음 명령을 입력합니다.

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAW
```

4. 다음 명령을 입력하여 **`MyAggregator`**라는 애그리게이터를 생성합니다.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

5. 입력을 눌러 명령을 실행합니다.

   다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

에 위임된 관리자 등록 AWS Config

위임된 관리자는 지정된 AWS 서비스에 대한 추가 관리 권한이 부여된 지정된 AWS 조직 내의 계정입니다. 자세한 내용은 AWS Organizations 사용 설명서의 위임된 관리자를 참조하세요. AWS CLI 을 사용하여 위임된 관리자를 등록할 수 있습니다.

위임된 관리자 등록

1. 관리 계정 자격 증명을 사용하여 로그인
2. 명령 프롬프트 또는 터미널 창을 엽니다.
3. 다음 명령을 입력하여 조직의 위임된 관리자로 서비스 액세스를 활성화하여 조직 전체에 AWS Config 규칙 및 적합성 팩을 배포하고 관리합니다.

   ```
   aws organizations enable-aws-service-access --service-principal=config-
   multiaccountsetup.amazonaws.com
   ```

4. 다음 명령을 입력하여 조직의 위임된 관리자로 서비스 액세스를 활성화하여 조직 전체의 AWS Config 데이터를 집계합니다.

   ```
   aws organizations enable-aws-service-access --service-
   principal=config.amazonaws.com
   ```

5. 서비스 액세스 활성화가 완료되었는지 확인하려면 다음 명령을 입력하고 Enter 키를 눌러 명령을 실행합니다.

```
aws organizations list-aws-service-access-for-organization
```

다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
            "DateEnabled": 1607020860.881
        }
    ]
}
```

6. 그런 다음, 다음 명령을 입력하여 멤버 계정을 AWS Config의 위임된 관리자로 등록합니다.

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

and

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. 위임된 관리자 등록이 완료되었는지 확인하려면 관리 계정에서 다음 명령을 입력하고 Enter 키를 눌러 명령을 실행합니다.

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

and

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::ManagementAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
        }
    ]
}
```

에 대한 집계자 편집 AWS Config

AWS Config 콘솔 또는를 사용하여 집계자를 AWS CLI 편집할 수 있습니다.

Editing Aggregators (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 애그리게이터 페이지로 이동하여 애그리게이터 이름을 선택합니다.
3. 작업을 선택하고 편집을 선택합니다.
4. 집계자 편집 페이지의 각 섹션을 사용하여 집계자의 소스 계정, IAM 역할 또는 리전을 변경합니다.

   > **Note**
   >
   > 소스 유형을 개별 계정에서 조직으로 또는 그 반대로 변경할 수 없습니다.

5. 저장을 선택합니다.

Editing Aggregators (AWS CLI)

1. `put-configuration-aggregator` 명령을 사용하여 구성 집계자를 업데이트 또는 편집할 수 있습니다.

   다음 명령을 입력하여 **MyAggregator**에 새 계정 ID를 추가합니다.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

2. 소스 계정에 따라 다음과 유사한 출력이 표시됩니다.

   개별 계정

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
        "CreationTime": 1517952090.769,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

   OR

   조직

```
{
    "ConfigurationAggregator": {
```

```
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

에 대한 집계자 삭제 AWS Config

AWS Config 콘솔 또는를 사용하여 집계자를 AWS CLI 삭제할 수 있습니다.

Deleting Aggregators (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 애그리게이터 페이지로 이동하여 애그리게이터 이름을 선택합니다.
3. 작업을 선택한 후 삭제를 선택합니다.

   경고 메시지가 표시됩니다. 집계자를 삭제하면 집계된 데이터가 모두 손실됩니다. 이 데이터는 복구할 수 없지만 소스 계정의 데이터는 영향을 받지 않습니다.
4. 삭제를 선택하여 선택 사항을 확인합니다.

Deleting Aggregators (AWS CLI)

다음 명령을 입력합니다.

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
 MyAggregator
```

명령이 성공하면 추가 출력이 표시되지 않습니다.

AWS Config 구성 및 규정 준수 데이터를 수집할 수 있도록 계정에 권한 부여

권한 부여는 AWS Config 구성 및 규정 준수 데이터를 수집하기 위해 애그리게이터 계정 및 리전에 부여하는 권한을 말합니다. AWS Organizations를 구성하는 소스 계정을 집계하는 경우에는 권한 부여가 필요하지 않습니다. AWS Config 콘솔 또는를 사용하여 집계자 계정을 승인 AWS CLI 할 수 있습니다.

주제

- 고려 사항
- 권한 부여 추가

고려 사항

애그리게이터는 개별 계정 애그리게이터와 조직 애그리게이터라는 두 가지 유형이 있습니다.

개별 계정 애그리게이터의 경우 외부 계정과 리전, 조직 멤버 계정과 리전 양쪽 모두를 비롯하여, 포함하려는 모든 소스 계정과 리전에 대한 권한 부여가 필요합니다.

조직 집계자의 경우 권한 부여가 AWS Organizations 서비스와 통합되므로 조직 멤버 계정 리전에는 권한이 필요하지 않습니다.

집계자는 사용자를 AWS Config 대신하여를 자동으로 활성화하지 않습니다.

AWS Config 소스 계정 및 리전에서 AWS Config 데이터를 생성하려면 두 유형의 애그리게이터에 대해 소스 계정 및 리전에서를 활성화해야 합니다.

권한 부여 추가

Adding Authorization (Console)

권한을 추가하여 애그리게이터 계정 및 리전에 AWS Config 구성 및 규정 준수 데이터를 수집할 수 있는 권한을 부여할 수 있습니다.

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 권한 부여 페이지로 이동하여 권한 추가를 선택합니다.
3. 집계자 계정에 집계자 계정의 12자리 계정 ID를 입력합니다.

4. 애그리게이터 리전의 경우, 애그리게이터 계정이 AWS Config 구성 및 규정 준수 데이터를 수집하도록 허용되는 AWS 리전 를 선택합니다.
5. 권한 부여를 선택하여 선택 사항을 확인합니다.

   AWS Config 에 집계자 계정, 리전 및 권한 부여 상태가 표시됩니다.

> **Note**
>
> AWS CloudFormation 샘플 템플릿을 사용하여 프로그래밍 방식으로 애그리게이터 계정 및 리전에 권한을 추가할 수도 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS::Config::AggregationAuthorization을 참조하세요.

Authorizing a Pending Request (Console)

기존 애그리게이터 계정의 권한 부여 요청이 보류 중인 경우 권한 부여 페이지에 요청 상태가 표시됩니다. 이 페이지에서 보류 상태의 요청을 승인할 수 있습니다.

1. 권한을 부여하려는 애그리게이터 계정을 선택한 다음, 권한 부여를 선택합니다.

   집계자 계정에이 계정에서 AWS Config 데이터를 수집할 수 있는 권한을 부여할 것인지 확인하는 확인 메시지가 표시됩니다.
2. 권한 부여를 다시 선택하여 애그리게이터 계정에 권한을 부여할 것인지 확인합니다.

   권한 상태가 권한 요청에서 권한 있음으로 바뀝니다.

권한 부여 승인 기간

개별 계정 애그리게이터에 소스 계정을 추가하려면 권한 부여 승인이 필요합니다. 보류 중인 권한 보유 승인 요청은 개별 계정 애그리게이터가 소스 계정을 추가한 후 7일 동안 제공됩니다.

Adding Authorization (AWS CLI)

1. 명령 프롬프트 또는 터미널 창을 엽니다.
2. 다음 명령을 입력합니다.

```
aws configservice put-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

3. 다음과 유사한 출력 화면이 표시되어야 합니다.

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

집계자 계정이 AWS Config 구성 및 규정 준수 데이터를 수집할 수 있는 권한 삭제

권한 부여는 AWS Config 구성 및 규정 준수 데이터를 수집하기 위해 애그리게이터 계정 및 리전에 부여하는 권한을 말합니다. AWS Organizations를 구성하는 소스 계정을 집계하는 경우에는 권한 부여가 필요하지 않습니다. AWS Config 콘솔 또는를 사용하여 권한 부여 AWS CLI 를 삭제할 수 있습니다.

주제

- 고려 사항
- 권한 부여 삭제

고려 사항

애그리게이터는 개별 계정 애그리게이터와 조직 애그리게이터라는 두 가지 유형이 있습니다.

개별 계정 애그리게이터의 경우 외부 계정과 리전, 조직 멤버 계정과 리전 양쪽 모두를 비롯하여, 포함하려는 모든 소스 계정과 리전에 대한 권한 부여가 필요합니다.

조직 집계자의 경우 권한 부여가 AWS Organizations 서비스와 통합되므로 조직 멤버 계정 리전에는 권한이 필요하지 않습니다.

집계자는 사용자를 AWS Config 대신하여를 자동으로 활성화하지 않습니다.

AWS Config 소스 계정 및 리전에서 AWS Config 데이터를 생성하려면 두 유형의 애그리게이터에 대해 소스 계정 및 리전에서를 활성화해야 합니다.

권한 부여 삭제

Deleting Authorization (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 권한 부여를 삭제하려는 애그리게이터 계정을 선택한 다음, 삭제를 선택합니다.

   경고 메시지가 표시됩니다. 이 권한을 삭제하면 AWS Config 데이터가 더 이상 집계자 계정과 공유되지 않습니다.
3. 삭제를 다시 선택하여 선택 사항을 확인합니다.

   이제 애그리게이터 계정이 삭제됩니다.

Deleting Authorization (AWS CLI)

다음 명령을 입력합니다.

```
aws configservice delete-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

명령이 성공하면 추가 출력이 표시되지 않습니다.

에 대한 집계자 보기 AWS Config

AWS Config 콘솔 또는를 사용하여 집계자를 AWS CLI 볼 수 있습니다.

Viewing Aggregators (Console)

에서 적합성 팩을 보려면 집계자 대시보드를 AWS Management Console참조하세요.

Viewing Aggregators (AWS CLI)

1. 다음 명령을 입력합니다.

   ```
   aws configservice describe-configuration-aggregators
   ```
2. 소스 계정에 따라 다음과 유사한 출력이 표시됩니다.

   개별 계정

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn":
 "arn:aws:config:Region:AccountID:config-aggregator/config-aggregator-floqpus3",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "MyAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

OR

조직

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

에 대한 다중 계정 다중 리전 데이터 집계 문제 해결 AWS Config

AWS Config 는 다음 이유 중 하나로 인해 소스 계정의 데이터를 집계하지 않을 수 있습니다.

이유	조치
AWS Config 는 조직 내 계정의 소스 계정에서 활성화되지 않습니다.	소스 계정 AWS Config 에서를 활성화하고 집계자 계정이 데이터를 수집하도록 승인합니다.
집계자 계정에 권한이 부여되지 않았습니다.	소스 계정에 로그인하고 집계자 계정에 AWS Config 데이터를 수집할 수 있는 권한을 부여합니다.
일시적 문제 때문에 데이터 집계가 금지될 수도 있습니다.	데이터 집계는 지연될 수 있습니다. 몇 분간 기다리십시오.

AWS Config 는 다음 이유 중 하나로 인해 조직의 데이터를 집계하지 않을 수 있습니다.

이유	조치
AWS Config 는 잘못된 IAM 역할로 인해 조직 세부 정보에 액세스할 수 없습니다.	IAM 역할을 생성하거나 IAM 역할 목록에서 유효한 IAM 역할을 선택합니다. **Note** IAM 역할이 7일 이상 유효하지 않은 경우는 전체 조직의 데이터를 AWS Config 삭제합니다.
AWS Config 조직에서 서비스 액세스가 비활성화되었습니다.	`EnableAWSServiceAccess` API를 AWS Organizations 통해 AWS Config 와 간의 통합을 활성화할 수 있습니다. 콘솔에서 내 조직 추가를 선택하면 AWS Config 가 및 간의 통합을 AWS Config 자동으로 활성화합니다 AWS Organizations.
AWS Config 조직에서 모든 기능이 활성화되지 않았기 때문에가 조직 세부 정보에 액세스할 수 없습니다.	AWS Organizations 콘솔에서 모든 기능을 활성화합니다.

이유	조치
계정 추가, 계정 제거, 서비스 액세스 활성화, 서비스 액세스 비활성화 등의 조직 변경 사항은 중동(바레인) 및 아시아 태평양(홍콩) 리전에서 즉시 업데이트되지 않습니다.	조직 변경 사항은 2시간 지연될 수 있습니다. 조직 변경 사항을 모두 보려면 2시간 정도 기다리시기 바랍니다.

를 사용하여 리소스의 AWS 현재 구성 상태 쿼리 AWS Config

일반 영어로 프롬프트를 입력하고 바로 사용 가능한 쿼리 형식으로 질문을 변환할 수 있는 생성형 인공 지능(생성형 AI) 기능을 사용하는 고급 쿼리용 미리 보기 기능이 도입되었습니다. 자세한 내용은 고급 쿼리용 자연어 쿼리 프로세서를 참조하세요.

AWS Config 를 사용하여 단일 계정 및 리전 또는 여러 계정 및 리전의 구성 속성을 기반으로 AWS 리소스의 현재 구성 상태를 쿼리할 수 있습니다. 가 AWS Config 지원하는 AWS 리소스 목록에서 현재 리소스 상태 메타데이터에 대해 속성 기반 쿼리를 수행할 수 있습니다. 지원되는 리소스 유형 목록에 대한 자세한 내용은 고급 쿼리에 지원되는 리소스 유형을 참조하세요.

고급 쿼리 기능은 서비스별로 Describe API 직접 호출을 수행하지 않고도 현재의 리소스 상태 메타데이터를 얻을 수 있는 단일 쿼리 엔드포인트 및 쿼리 언어를 제공합니다. 구성 집계자를 사용하여 여러 계정 및 AWS 리전의 중앙 계정에서 동일한 쿼리를 실행할 수 있습니다.

주제

- Features
- 에 대한 쿼리 구성 요소 AWS Config
- 용 SQL 쿼리 편집기를 사용한 쿼리 AWS Config (콘솔)
- (AWS CLI)용 AWS Config SQL 쿼리 편집기를 사용한 쿼리
- AWS Config 고급 쿼리를 위한 자연어 쿼리 프로세서
- 에 대한 쿼리 예제 AWS Config
- AWS Config예제 관계 쿼리
- 제한 사항
- 고급 쿼리에 대한 CIDR 표기법/IP 범위 동작
- 고급 쿼리에 대한 배열 동작 내의 여러 속성
- 리전 지원

Features

AWS Config 는 구조화된 쿼리 언어(SQL) SELECT 구문의 하위 집합을 사용하여 현재 구성 항목(CI) 데이터에 대한 속성 기반 쿼리 및 집계를 수행합니다. 쿼리는 태그 및/또는 리소스 식별자에 대한 단순 확

인부터 버전 관리가 비활성화된 모든 Amazon S3 버킷 확인까지 다양한 범위를 지원합니다. 이를 통해 AWS 서비스별 API 호출을 수행하지 않고도 필요한 현재 리소스 상태를 정확히 쿼리할 수 있습니다.

`AVG`, `COUNT`, `MAX`, `MIN`, `SUM` 등의 집계 함수를 지원합니다.

고급 쿼리를 사용할 수 있는 경우:

- 인벤토리 관리(예: 특정 크기의 Amazon EC2 인스턴스 목록 가져오기)
- 보안 및 지능형 운영(예: 특정한 구성 속성이 활성화 또는 비활성화된 리소스 목록 가져오기)
- 비용 최적화(예: EC2 인스턴스에 연결되지 않은 Amazon EBS 볼륨 목록 식별)
- 규정 준수 데이터(예: 모든 적합성 팩 및 그것들의 규정 준수 상태 목록 가져오기)

AWS SQL 쿼리 언어를 사용하는 방법에 대한 자세한 내용은 SQL(구조화된 쿼리 언어)이란 무엇입니까?를 참조하세요.

에 대한 쿼리 구성 요소 AWS Config

AWS Config 고급 `SELECT` 쿼리의 SQL 쿼리 구성 요소는 다음과 같습니다.

시놉시스

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

파라미터

[WHERE condition]

지정한 `condition`에 따라 결과를 필터링합니다.

비교 연산자

- = (같음)
- `IN` (멤버십 나열)
- `BETWEEN` (범위 확인)

로직 연산자

- AND
- OR
- NOT

[GROUP BY 속성]

결과를 지정된 속성에 대한 일치 값이 포함된 행 그룹으로 집계합니다.

GROUP BY 절은 집계에 적용됩니다.

[ORDER BY 속성 [ASC | DESC] [, 속성 [ASC | DESC] ...]]

하나 이상의 출력 properties으로 결과 집합을 정렬합니다.

절에 여러 개의 속성이 포함되어 있을 때는 결과 집합이 첫 번째 property에 따라 정렬된 다음, 첫 번째 속성과 일치하는 값을 가진 행에 대해서는 두 번째 property가 적용되는 등의 방식이 적용됩니다.

예시

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

용 SQL 쿼리 편집기를 사용한 쿼리 AWS Config (콘솔)

> 일반 영어로 프롬프트를 입력하고 바로 사용 가능한 쿼리 형식으로 질문을 변환할 수 있는 생성형 인공 지능(생성형 AI) 기능을 사용하는 고급 쿼리용 미리 보기 기능이 도입되었습니다. 자세한 내용은 고급 쿼리용 자연어 쿼리 프로세서를 참조하세요.

AWS 샘플 쿼리를 사용하거나 사용자 지정 쿼리라고 하는 자체 쿼리를 생성할 수 있습니다.

고려 사항

사전 조건

다음 AWS 관리형 정책 중 하나를 사용하는 경우 쿼리를 실행하고 저장하는 데 필요한 권한이 있습니다. AWSServiceRoleForConfig(서비스 연결 역할) 또는 AWS_ConfigRole.

그렇지 않으면 AWSConfigUserAccess AWS 관리형 정책에 권한이 포함되어야 합니다.

쿼리할 수 있는 속성 목록

속성 및 해당 데이터 유형의 업데이트된 목록은 GitHub에서 찾을 수 있습니다.

고급 쿼리 및 애그리게이터

집계기에서 쿼리를 실행하려면 집계기를 만듭니다. 자세한 내용은 에 대한 집계자 생성 AWS Config 섹션을 참조하세요.

이미 집계기가 설정되어 있는 경우 쿼리 범위에서 그 집계기를 선택하고 그 집계기에 대해 고급 쿼리를 실행합니다. 집계자를 선택할 때는 쿼리 문에 AWS 계정 ID와 AWS 리전을 추가하여 결과에서 해당 정보를 보는 것이 좋습니다.

AWS 샘플 쿼리 사용

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 왼쪽 탐색 메뉴에서 고급 쿼리를 선택하여 단일 계정 및 지역 또는 여러 계정 및 지역의 리소스 구성을 쿼리할 수 있습니다.
3. 고급 쿼리 페이지의 쿼리 목록에서 적절한 쿼리를 선택합니다. 이름, 설명, 작성자 또는 태그별로 쿼리 목록을 필터링할 수 있습니다. AWS 쿼리를 필터링하려면 작성자를 선택한 후 AWS를 입력합니다. 선택한 쿼리가 SQL 쿼리 편집기에 표시됩니다. 선택한 쿼리를 필요에 맞게 편집할 수 있습니다.
4. 이 쿼리를 새 쿼리에 저장하려면 다른 이름으로 저장을 선택합니다.
   - 쿼리 이름 필드에서 쿼리 이름을 업데이트합니다.
   - 설명 필드에서 쿼리의 설명을 업데이트합니다.
   - 이 쿼리에 최대 50개의 고유 태그를 입력합니다.
   - 저장을 선택합니다.
5. Run(실행)을 선택합니다. 쿼리 결과는 쿼리 편집기 아래 테이블에 표시됩니다.
6. 쿼리 결과를 CSV 또는 JSON 형식으로 내보내려면 내보내기 형식을 선택합니다.

사용자 정의 쿼리 생성

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.

2. 왼쪽 탐색 메뉴에서 고급 쿼리를 선택하여 단일 계정 및 지역 또는 여러 계정 및 지역의 리소스 구성을 쿼리할 수 있습니다.
3. 자체 쿼리를 만들려면 새 쿼리를 선택합니다.

   사용자 지정 쿼리를 보거나 편집하려면 이름, 설명, 생성자 또는 태그별로 쿼리를 필터링합니다. 사용자 지정 쿼리를 필터링하려면 생성자를 선택한 후 사용자 지정을 입력합니다.
4. 쿼리 편집기 페이지에서 이 계정과 리전에 대한 자체 쿼리를 만듭니다. 적절한 집계기를 선택하여 여러 계정 및 리전에 대한 쿼리를 만들 수도 있습니다.
5. 이 쿼리를 수정하려면 편집합니다. 이 쿼리를 저장하려면 쿼리 저장을 선택합니다.

   - 쿼리 이름 필드에서 쿼리 이름을 업데이트합니다.
   - 설명 필드에서 쿼리의 설명을 업데이트합니다.
   - 이 쿼리에 최대 50개의 고유 태그를 입력합니다.
   - 저장을 선택합니다.
6. Run(실행)을 선택합니다. 쿼리 결과는 쿼리 편집기 아래 테이블에 표시됩니다.
7. 쿼리 결과를 CSV 또는 JSON 형식으로 내보내려면 내보내기 형식을 선택합니다.

(AWS CLI)용 AWS Config SQL 쿼리 편집기를 사용한 쿼리

AWS CLI 는 AWS 서비스를 관리하기 위한 통합 도구입니다. 다운로드 및 구성할 도구를 하나만 사용하면 명령줄에서 여러 AWS 서비스를 제어하고 스크립트를 사용하여 자동화할 수 있습니다. AWS CLI 및에 대한 자세한 내용과 AWS CLI 도구 설치 지침은 AWS Command Line Interface 사용 설명서의 다음을 참조하세요.

- AWS Command Line Interface 사용 설명서
- AWS Command Line Interface를 이용한 설정

필요한 경우 `aws configure`를 입력하여 고급 쿼리를 사용할 수 있는 리전 AWS CLI 을 사용하도록 를 AWS 구성합니다.

고려 사항

사전 조건

다음 AWS 관리형 정책 중 하나를 사용하는 경우 AWSServiceRoleForConfig(서비스 연결 역할) 또는 AWSAWS_ConfigRole 쿼리를 실행하고 저장하는 데 필요한 권한이 있습니다.

그렇지 않으면 AWSConfigUserAccess AWS 관리형 정책에 권한이 포함되어야 합니다.

쿼리할 수 있는 속성 목록

속성 및 해당 데이터 유형의 업데이트된 목록은 GitHub에서 찾을 수 있습니다.

고급 쿼리 및 애그리게이터

집계기에서 쿼리를 실행하려면 집계기를 만듭니다. 자세한 내용은 에 대한 집계자 생성 AWS Config 섹션을 참조하세요.

이미 집계기가 설정되어 있는 경우 쿼리 범위에서 그 집계기를 선택하고 그 집계기에 대해 고급 쿼리를 실행합니다. 집계자를 선택할 때는 쿼리 문에 AWS 계정 ID와 AWS 리전을 추가하여 결과에서 해당 정보를 보는 것이 좋습니다.

리소스 구성 데이터 쿼리

단일 계정 및 리전에 대해 쿼리 편집기(AWS CLI)를 사용하여 리소스 구성 데이터를 쿼리하려면

1. 명령 프롬프트 또는 터미널 창을 엽니다.
2. 다음 명령을 입력하여 리소스 환경 데이터를 쿼리합니다.

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

쿼리에 따라 다음과 같은 내용이 출력됩니다.

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
```

```
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

여러 계정 및 리전에 대해 쿼리 편집기(AWS CLI)를 사용하여 리소스 구성 데이터를 쿼리하려면

1. 명령 프롬프트 또는 터미널 창을 엽니다.
2. 다음 명령을 입력하여 리소스 환경 데이터를 쿼리합니다.

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

쿼리에 따라 다음과 같은 내용이 출력됩니다.

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

> **Note**
>
> 고급 쿼리에 `AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role`, `AWS::IAM::Policy` 리소스 유형을 사용하는 경우, `awsRegion = 'global'`을 사용하세요.

쿼리를 저장합니다.

1. 명령 프롬프트 또는 터미널 창을 엽니다.
2. 다음 명령을 입력하여 쿼리를 저장합니다.

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. 쿼리에 따라 다음과 같은 내용이 출력됩니다.

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags`은 선택 사항입니다. 태그를 전달하면 `list-stored-queries` 또는 `get-stored-query` 어느 쪽에서도 저장된 태그가 반환되지 않습니다. 저장된 쿼리의 관련 태그를 검색하려면 `list-tag-for-resources`를 사용해야 합니다.
> 쿼리를 만들거나 업데이트할 때는 `--description`는 선택 사항입니다.

저장된 모든 쿼리 보기

1. 다음 명령을 입력하여 저장된 쿼리의 전체 목록을 봅니다.

```
aws configservice list-stored-queries
```

2. 쿼리에 따라 다음과 같은 내용이 출력됩니다.

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
```

```
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
    ]
}
}
```

저장된 쿼리의 세부 정보 조회

1. 다음 명령을 입력하여 저장된 특정 쿼리의 세부정보를 확인합니다.

```
aws configservice get-stored-query --query-name cli-test
```

2. 쿼리에 따라 다음과 같은 내용이 출력됩니다.

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

저장된 쿼리 삭제

- 다음 명령을 입력하여 저장한 쿼리를 삭제합니다.

```
aws configservice delete-stored-query --query-name cli-test
```

명령이 성공하면 추가 출력이 표시되지 않습니다.

AWS Config 고급 쿼리를 위한 자연어 쿼리 프로세서

> 고급 쿼리의 자연어 쿼리 프로세서는에 대한 평가판 릴리스 AWS Config 이며 변경될 수 있습니다.

고급 쿼리용 자연어 쿼리 프로세서는 일반 영어로 프롬프트를 입력한 후 바로 사용 가능한 쿼리 형식으로 질문을 변환할 수 있는 생성형 인공 지능(생성형 AI) 기술인 Amazon Bedrock을 사용합니다. 자연어 쿼리 프로세서를 사용하면 AWS 조직 전체에서 AWS 계정 또는를 쿼리할 수 있습니다.

프롬프트트는 의문형 또는 평서문일 수 있습니다. 예를 들어 'Which load balancers are created after January 1, 2024?' 또는 ‘List all my lambda function that is running node js 16.’과 같은 프롬프트를 입력할 수 있습니다.

고려 사항

자연어 쿼리 프로세서는 다음 작업을 수행할 수 없습니다.

- 영어 이외의 언어로 쿼리 생성
- 고급 쿼리와 관련이 없는 프롬프트에 대한 쿼리 생성
- 1,000자 이상의 프롬프트에 대한 쿼리 생성
- 후속 수정 또는 이전 세션에 대한 쿼리 생성
- 생성된 코드 설명

자연어 쿼리 프로세서를 사용한 쿼리

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 왼쪽 탐색 메뉴에서 고급 쿼리를 선택하여 단일 계정 및 지역 또는 여러 계정 및 지역의 리소스 구성을 쿼리할 수 있습니다.
3. 고급 쿼리 페이지에서 새 쿼리를 선택하여 쿼리 편집기로 이동합니다.
    - 애그리게이터로 쿼리를 실행하려면 애그리게이터를 생성합니다. 자세한 내용은 에 대한 집계자 생성 AWS Config 섹션을 참조하세요.

- 이미 애그리게이터를 설정한 경우 쿼리 범위에서 그 애그리게이터를 선택하고 그 애그리게이터에 대해 고급 쿼리를 실행합니다. 집계자를 선택할 때는 쿼리 문에 AWS 계정 ID 및 AWS 리전을 추가하여 결과에서 해당 정보를 보는 것이 좋습니다.

4. 쿼리 편집기에서 자연어 쿼리 프로세서 섹션으로 이동합니다. 일반 영어로 프롬프트를 입력한 다음 생성을 선택합니다. 예제는 프롬프트 예제를 참조하세요.
5. 쿼리를 생성한 후 복사(기능적으로는 Ctrl+C와 동일)를 선택하여 쿼리를 클립보드에 복사하거나 편집기에 채우기를 선택할 수 있습니다. 편집기에 채워진 경우 생성된 쿼리를 필요에 맞게 편집할 수 있습니다.
6. 이 쿼리를 새 쿼리에 저장하려면 다른 이름으로 저장을 선택합니다.
   - 쿼리 이름 필드에서 쿼리 이름을 업데이트합니다.
   - 설명 필드에서 쿼리의 설명을 업데이트합니다.
   - 이 쿼리에 최대 50개의 고유 태그를 입력합니다.
   - 저장을 선택합니다.
7. Run(실행)을 선택합니다. 쿼리 결과는 쿼리 편집기 아래 테이블에 표시됩니다.
8. 쿼리 결과를 CSV 또는 JSON 형식으로 내보내려면 내보내기 형식을 선택합니다.

> **Note**
> 쿼리 결과가 페이지 매김됩니다. 내보내는 경우 최대 500개의 결과가 내보내집니다. API를 사용하여 모든 결과를 검색할 수도 있습니다. 결과는 페이지 매김되며 한 번에 100개의 결과를 검색할 수 있습니다.

프롬프트 예제

다음은 예제로 사용할 수 있는 프롬프트와 생성 쿼리입니다.

Example: What load balancers were created after January 1, 2024?

프롬프트

생성된 쿼리:

```
SELECT
    resourceId,
```

```
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
    resourceCreationTime
DESC
```

Example: Which of my RDS database instances are publicly accessible?

프롬프트

생성된 쿼리:

```
SELECT
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: How many EC2 instances were created in last one year?

프롬프트

생성된 쿼리:

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
AND
    '2024-05-10T16:56:25.000Z'
```

Example: How many EC2 instances do I have in each of my AWS 계정?

프롬프트

생성된 쿼리:

```
SELECT
    accountId,
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: Which IAM roles have the managed policy AdministratorAccess attached?

프롬프트

생성된 쿼리:

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: EBS volumes without encryption

프롬프트

생성된 쿼리:

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.encrypted = false
```

Example: Get noncompliant resources

프롬프트

생성된 쿼리:

```
SELECT
    resourceId,
    resourceType
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: List all my lambda function that is running node js 16

프롬프트

생성된 쿼리:

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: What ACM certificates expire the next 30 days?

프롬프트

생성된 쿼리:

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
```

```
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53'
```

> **Note**
> 생성된 쿼리의 시간은 프롬프트를 입력한 시간에 따라 달라집니다.

피드백 제공

자연어 쿼리 프로세서에 대한 전반적인 피드백 또는 생성된 특정 쿼리에 대한 피드백을 제공할 수 있습니다.

자연어 쿼리 프로세서에 대한 피드백 제공

오른쪽의 자연어 쿼리 프로세서 위에 나타나는 피드백 제공 버튼을 선택합니다. 만족 또는 불만족을 입력하고가 자연어 쿼리를 더 유용하게 만들 수 있는 방법에 대한 피드백을 제공할 AWS Config 수 있습니다.

> **Note**
> 개인 정보, 상업적으로 민감한 정보 또는 기밀 정보를 공개하지 마세요.

생성된 특정 쿼리에 대한 피드백 제공

생성된 쿼리 아래에 나타나는 좋아요 또는 싫어요 버튼을 선택하여 생성된 쿼리에 대한 피드백을 제공할 수 있습니다.

리전 지원

자연어 쿼리 프로세서는 다음 리전에서 지원됩니다.

리전 이름	지역	엔드포인트	프로토콜
미국 동부 (버지니아 북부)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
미국 서부 (오레곤)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

에 대한 쿼리 예제 AWS Config

다음 쿼리 예제를 봅니다.

Query to list all EC2 instances with AMI ID ami-12345

쿼리:

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

결과:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
```

```
            },
            {
                "Name": "configuration.imageId"
            },
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

Query for count of resources grouped by their AWS Config rules compliance status

쿼리:

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
```

```
    configuration.complianceType
```

결과:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of AWS Conformance packs

쿼리:

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

결과:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
```

```
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of AWS resources grouped by account ID

쿼리:

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

결과:

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
```

```
                "Name": "accountId"
            }
        ]
    }
}
```

Query to list all EC2 volumes that are not in use

쿼리:

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

결과:

```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
```

```
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
```

```
}
```

AWS Config예제 관계 쿼리

다음 예제 관계 쿼리를 봅니다.

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

OR

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
```

```
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

제한 사항

> **Note**
>
> 고급 쿼리는 구성 레코더에서 기록하도록 구성되지 않은 리소스에 대한 쿼리를 지원하지 않습니다.는 리소스가 검색되었지만 구성 레코더에서 기록하도록 구성되지 않은 `configurationItemStatus` 경우 `ResourceNotRecorded`에서를 사용하여 구성

항목(CIs)을 AWS Config 생성합니다. 집계자는 이러한 CI를 집계하지만 고급 쿼리는 `ResourceNotRecorded`를 사용한 CI 쿼리를 지원하지 않습니다. 쿼리하려는 리소스 유형을 기록하려면 레코더 설정을 업데이트하세요.

SQL `SELECT`의 하위 집합인 쿼리 구문에는 다음과 같은 제한 사항이 있습니다.

- 쿼리에서`ALL`, `AS`, `DISTINCT`, `FROM`, `HAVING`, `JOIN`, 및 `UNION` 키워드는 지원되지 않습니다. `NULL` 값 쿼리는 지원되지 않습니다.
- 쿼리에서 직접 우선 순위 필드를 생성하기 위한 복잡한 `CASE` 문을 지원하지 않습니다.
- 타사 리소스에 대한 쿼리는 지원되지 않습니다. 고급 쿼리를 사용하여 검색한 타사 리소스의 구성 필드는 `NULL`로 설정됩니다.
- SQL 쿼리로 중첩 구조(예: 태그)의 팩킹을 해제하는 기능은 지원되지 않습니다.
- 삭제된 리소스 쿼리는 지원되지 않습니다. 삭제된 리소스를 검색하려면 검색한 리소스 조회를 참조하세요 AWS Config.
- 모든 열 `SELECT` 약칭(`SELECT *`)이 CI의 최상위 스칼라 속성만 선택합니다. 반환되는 스칼라 속성은 `accountId`, `awsRegion`, `arn`, `availabilityZone`, `configurationItemCaptureTime`, `resourceCreationTime`, `resourceId`, `resourceName`, `resourceType` 및 `version`입니다.
- 와일드카드 제한 사항:
  - 와일드카드는 속성 키가 아닌 속성 값에 대해서만 지원됩니다(예를 들어 `...WHERE someKey LIKE 'someValue%'`는 지원되지만 `...WHERE 'someKey%' LIKE 'someValue%'`는 지원되지 않음).
  - 접미사 와일드카드에 대해서만 지원됩니다(예를 들어 `...LIKE 'AWS::EC2::%'` 및 `...LIKE 'AWS::EC2::_'`는 지원되지만 `...LIKE '%::EC2::Instance'` 및 `...LIKE '_::EC2::Instance'`는 지원되지 않음).
  - 와일드카드 일치 항목의 길이는 최소 세 문자여야 합니다(예를 들어 `...LIKE 'ab%'` 및 `...LIKE 'ab_'`는 허용되지 않지만 `...LIKE 'abc%'` 및 `...LIKE 'abc_'`는 허용됩니다).

  > **Note**
  >
  > `'_'`(단일 밑줄)도 와일드카드로 취급됩니다.

- 집계 제한 사항:
  - 집계 함수에는 단일 인수 또는 속성만 사용할 수 있습니다.
  - 집계 함수에는 인수 같은 다른 함수를 사용할 수 없습니다.

  - 집계 함수를 참조하는 ORDER BY 절을 사용한 GROUP BY는 단일 속성만 포함할 수 있습니다.
  - 다른 모든 집계 GROUP BY 절의 경우 최대 세 개의 속성을 포함할 수 있습니다.
  - ORDER BY 절에 집계 함수가 있는 경우를 제외하고 모든 집계 쿼리에서 페이지 매김이 지원됩니다. 예를 들어 Y가 집계 함수인 경우 GROUP BY X, ORDER BY Y는 작동하지 않습니다.
  - 집계에서 HAVING 절을 지원하지 않습니다.
- 일치하지 않는 식별자 제한 사항:

  일치하지 않는 식별자는 철자는 같지만 대/소문자(대문자 및 소문자)가 다른 속성입니다. 고급 쿼리는 일치하지 않는 식별자가 포함된 쿼리를 처리할 수 없습니다. 예시:

  - 철자는 같지만 대/소문자가 다른 두 속성(configuration.dbclusterIdentifier 및 configuration.dBClusterIdentifier)
  - 한 속성이 다른 속성의 하위 집합이고 대/소문자가 다른 두 속성(configuration.ipAddress 및 configuration.ipaddressPermissions)

고급 쿼리에 대한 CIDR 표기법/IP 범위 동작

CIDR 표기법은 검색을 위해 IP 범위로 변환됩니다.

즉, "=" 및 "BETWEEN"는 정확한 IP 대신 제공된 IP를 포함하는 모든 범위를 검색합니다.

정확한 IP 범위를 검색하려면 범위를 벗어난 IP를 제외하는 벌도의 조건을 추가해야 합니다.

Example 정확한 CIDR 블록 10.0.0.0/24 검색

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

Example 정확한 IP 주소 192.168.0.2/32 검색

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

고급 쿼리에 대한 배열 동작 내의 여러 속성

객체 배열 내의 여러 속성을 쿼리할 때 모든 배열 요소에 대해 일치 항목이 계산됩니다.

예를 들어, 규칙 A와 B가 있는 리소스 R의 경우, 리소스가 규칙 A를 준수하지만 규칙 B는 준수하지 않는 경우 리소스 R은 다음과 같이 저장됩니다.

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

다음 쿼리로 R이 반환됩니다.

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

첫 번째 조건은 R.configRuleList의 모든 요소에 `configuration.configRuleList.complianceType = 'non_compliant'` 적용됩니다. R에는 complianceType = 'non_compliant'인 규칙(규칙 B)이 있으므로 조건은 true로 평가됩니다.

두 번째 조건은 R.configRuleList의 모든 요소에 `configuration.configRuleList.configRuleName` 적용됩니다. R에는 configRuleName = 'A'인 규칙(규칙 A)이 있으므로 조건이 true로 평가됩니다. 두 조건이 모두 true면 R이 반환됩니다.

리전 지원

고급 쿼리는 다음 리전에서 지원됩니다.

리전 이름	지역	엔드포인트	프로토콜	
미국 동부(오하이오)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
미국 동부(버지니아 북부)	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
미국 서부(캘리포니아 북부)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
미국 서부(오레곤)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
아프리카(케이프타운)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
아시아 태평양(홍콩)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
아시아 태평양(하이데라바드)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
아시아 태평양(자카르타)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
아시아 태평양(말레이시아)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS	

리전 이름	지역	엔드포인트	프로토콜
아시아 태평양(멜버른)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
아시아 태평양(뭄바이)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
아시아 태평양(오사카)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
아시아 태평양(서울)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
아시아 태평양(싱가포르)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
아시아 태평양(시드니)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
아시아 태평양(타이베이)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
아시아 태평양(태국)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
아시아 태평양(도쿄)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
캐나다(중부)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
캐나다 서부(캘거리)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
유럽(프랑크푸르트)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
유럽(아일랜드)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
유럽(런던)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
유럽(밀라노)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
유럽(파리)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
유럽(스페인)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
유럽(스톡홀름)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
유럽(취리히)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
이스라엘(텔아비브)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
멕시코(중부)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS

리전 이름	지역	엔드포인트	프로토콜
중동(바레인)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
중동 (UAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
남아메리카(상파울루)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 동부)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud(미국 서부)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config 데이터 삭제

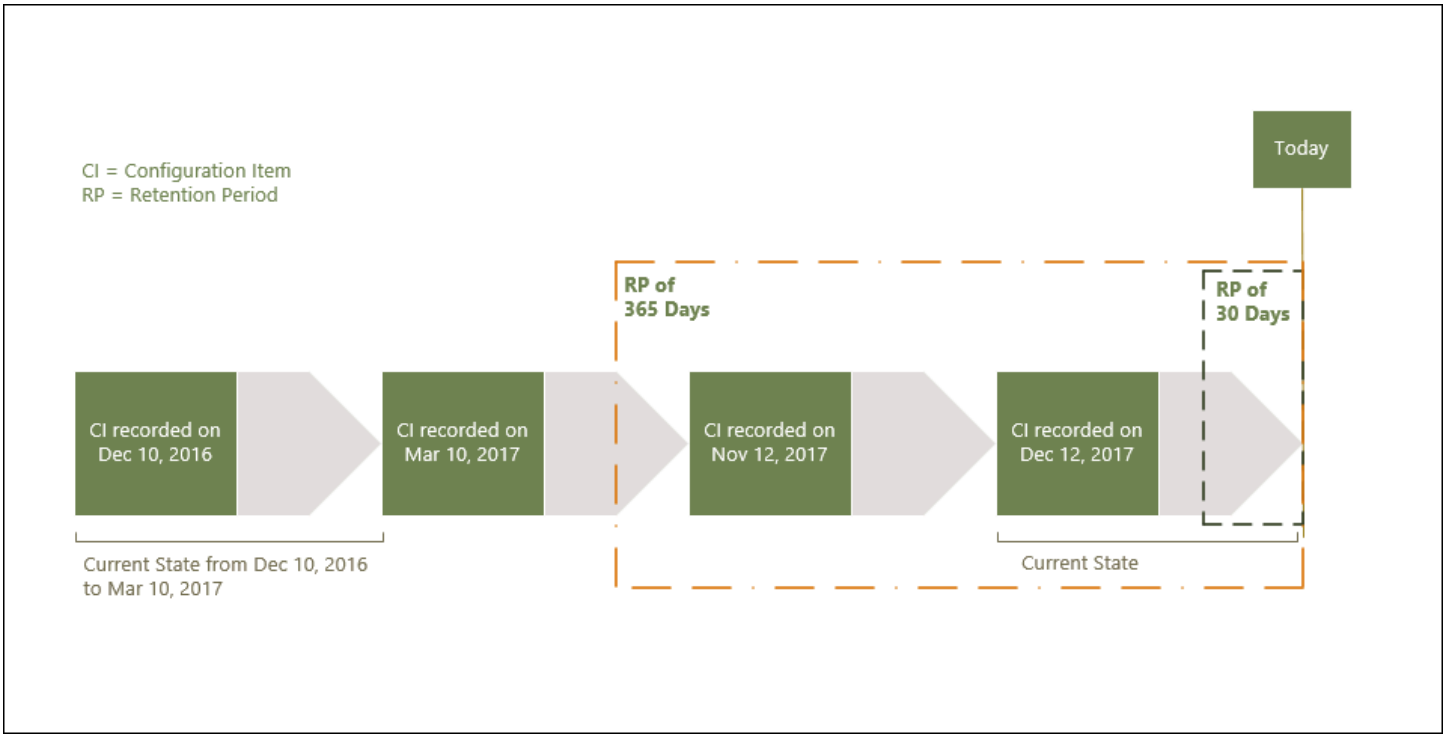
> **Note**
>
> AWS Config 는 구성 스냅샷 및 구성 기록 파일을 보내기 위해 Amazon Simple Storage Service(Amazon S3) 및 Amazon Simple Notification Service(Amazon SNS)를 사용하지만 에는 자체 데이터 스토어 및 보존 정책 AWS Config 이 있습니다. 이 페이지의 정보는에 고유합니다 AWS Config. Amazon S3 및 Amazon SNS에는 별도의 데이터 스토어 및 보존 정책이 있습니다.

AWS Config 를 사용하면에 대한 보존 기간을 지정하여 데이터를 삭제할 수 있습니다`ConfigurationItems`. 보존 기간을 지정하면는 지정된 기간 `ConfigurationItems` 동안를 AWS Config 유지합니다. 최소 30일에서 최대 7년(2557일) 사이의 기간을 선택할 수 있습니다. 는 지정된 보존 기간보다 오래된 데이터를 AWS Config 삭제합니다. 보존 기간을 지정하지 않는 경우 AWS Config 는 7년(2557일)의 기본 기간 동안 `ConfigurationItems`를 계속 저장합니다. 기록이 켜져 있으면 리소스의 현재 상태는 `ConfigurationItem`이 기록될 때 및 다음 변경(새 `ConfigurationItem`)이 기록될 때까지 입니다.

보존 기간 동작을 이해하려면 타임라인을 살펴보겠습니다.

- 기록이 켜져 있으면 리소스의 현재 상태는 항상 존재하며 `ConfigurationItem`이 기록되는 날짜와 관계없이 삭제할 수 없습니다.
- 가 새 `ConfigurationItems`를 AWS Config 기록하면 지정된 보존 기간에 따라 이전 `ConfigurationItems`이 삭제됩니다.

다음 타임라인에서는 `ConfigurationItems` 다음 날짜를 AWS Config 기록합니다. 이 타임라인의 목적상 오늘은 2018년 5월 24일 표시됩니다.



다음 테이블은 선택된 보존 기간에 근거하여 AWS Config 타임라인에 표시되는 `ConfigurationItems`를 설명합니다.

보존 기간	타임라인에서 표시되는 구성 항목	설명
30일	2017년 12월 12일	현재 리소스 상태는 `ConfigurationItem` 이 기록된 2017년 12월 12일부터 시작하며 오늘(2018년 5월 24일)까지 유효합니다. 기록이 켜져 있으면 현재 상태는 항상 존재합니다.
365일	2017년 12월 12일, 2017년 11월 12일, 2017년 3월 10일	보존 기간은 2017년 12월 12일 현재 상태와 이전 `ConfigurationItems` 2017년 11월 12일과 2017년 3월 10일을 보여줍니다. 구성 상태가 365일 전 현재 상태를 표시하였기 때문에 2017년 3월 10일의 `ConfigurationItem` 이 타임라인에 표시됩니다.

보존 기간을 지정하면 AWS Config APIs는 지정된 보존 기간보다 오래된 상태를 `ConfigurationItems` 나타내는를 더 이상 반환하지 않습니다.

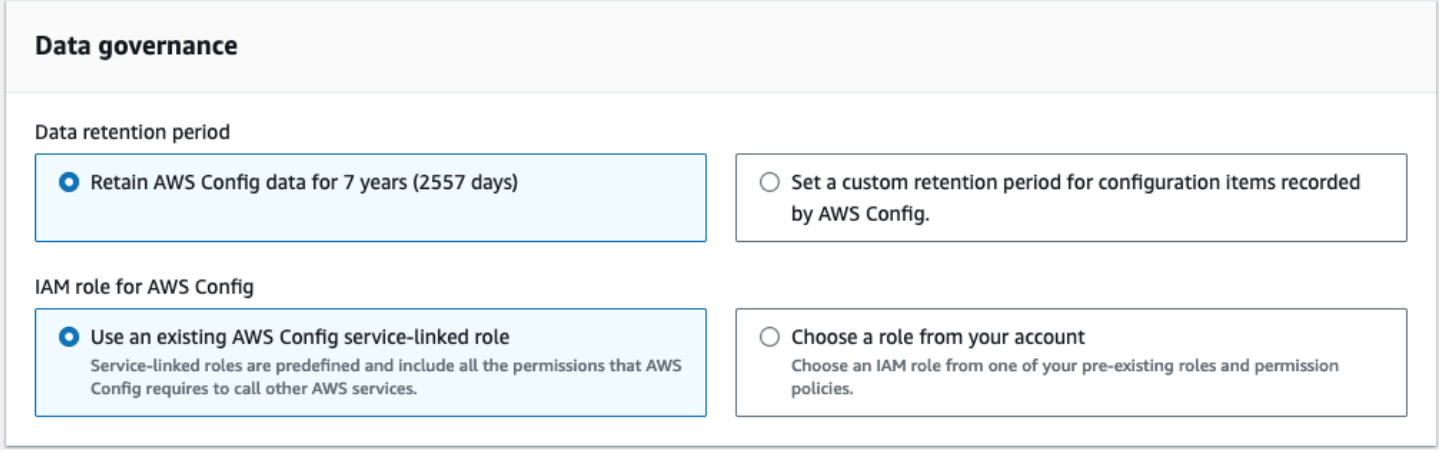
> **Note**
>
> - AWS Config 녹음이 꺼져 `ConfigurationItems` 있으면가를 녹음할 수 없습니다.
> - AWS Config IAM 역할에 권한이 충분하지 않은 `ConfigurationItems` 경우는를 기록할 수 없습니다. 자세한 내용은 할당된 IAM 역할에 대한 권한을 참조하세요 AWS Config.

에서 데이터 보존 기간 설정 AWS Management Console

에서 데이터 보존 기간을 선택하지 AWS Management Console않으면 기본 기간은 7년 또는 2557일입니다.

구성 항목의 사용자 지정 데이터 보존 기간을 설정하려면 확인란을 선택합니다. 1년, 3년, 5년 또는 사용자 지정 기간을 선택할 수 있습니다. 사용자 지정 기간의 경우 30일 ~ 2557일 사이의 일수를 입력합니다.

다음 이미지는 데이터 거버넌스 에서 데이터 보존 기간을 설정할 수 있는 위치에 표시됩니다. 왼쪽 탐색 모음에서 설정을 선택한 다음 편집을 선택하여 콘솔의 설정 편집 페이지에서 데이터 거버넌스에 액세스할 수 있습니다. AWS Config



의 보안 AWS Config

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 클라우드에서 AWS AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. 에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 제공 범위 내 서비스를 AWS Config참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다 AWS Config. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 AWS Config 를 구성하는 방법을 보여줍니다.

주제

- 의 데이터 보호 AWS Config
- 에 대한 자격 증명 및 액세스 관리 AWS Config
- 의 인시던트 대응 AWS Config
- 에 대한 규정 준수 검증 AWS Config
- 의 복원력 AWS Config
- 의 인프라 보안 AWS Config
- 교차 서비스 혼동된 대리자 방지
- 에 대한 보안 모범 사례 AWS Config

의 데이터 보호 AWS Config

AWS 공동 책임 모델 AWS Config의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되

는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Config 또는 기타 AWS AWS 서비스 에서 콘솔, API AWS CLI또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

저장된 데이터 암호화

저장 데이터는 투명 서버 측 암호화를 사용하여 암호화됩니다. 이를 사용하면 중요한 데이터 보호와 관련된 운영 부담 및 복잡성을 줄일 수 있습니다. 유휴 시 암호화를 사용하면 암호화 규정 준수 및 규제 요구 사항이 필요한, 보안에 민감한 애플리케이션을 구축할 수 있습니다.

전송 중인 데이터 암호화

에서 수집하고 액세스하는 데이터는 전송 계층 보안(TLS) 보호 채널을 통해서만 AWS Config 제공됩니다.

에 대한 자격 증명 및 액세스 관리 AWS Config

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 누가 AWS Config 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

- 대상
- ID를 통한 인증
- 정책을 사용하여 액세스 관리
- AWS Config 에서 IAM을 사용하는 방법
- 에 대한 자격 증명 기반 정책 예제 AWS Config
- AWS 에 대한 관리형 정책 AWS Config
- 에 할당된 IAM 역할에 대한 권한 AWS Config
- 고객 관리형 구성 레코더의 IAM 역할 업데이트
- AWS Config 전송 채널에 대한 Amazon S3 버킷에 대한 권한
- AWS Config 전송 채널의 KMS 키에 대한 권한
- Amazon SNS 주제에 대한 권한
- AWS Config 자격 증명 및 액세스 문제 해결
- 에 서비스 연결 역할 사용 AWS Config

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 수행하는 작업에 따라 다릅니다 AWS Config.

서비스 사용자 - AWS Config 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 AWS Config 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니

다. AWS Config의 기능에 액세스할 수 없는 경우 AWS Config 자격 증명 및 액세스 문제 해결을 참조하세요.

서비스 관리자 - 회사에서 AWS Config 리소스를 책임지고 있는 경우에 대한 전체 액세스 권한을 가지고 있을 것입니다 AWS Config. 서비스 관리자는 서비스 사용자가 액세스해야 하는 AWS Config 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가에서 IAM을 사용하는 방법에 대한 자세한 내용은 섹션을 AWS Config참조하세요AWS Config 에서 IAM을 사용하는 방법.

IAM 관리자 - IAM 관리자라면 AWS Config에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 자격 AWS Config 증명 기반 정책 예제를 보려면 섹션을 참조하세요에 대한 자격 증명 기반 정책 예제 AWS Config.

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. IAM 사용자 또는 AWS 계정 루트 사용자 IAM 역할을 수임하여 로 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어는 멀티 팩터 인증(MFA)을 사용하여 계정의 보안을 강화할 것을 AWS 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는

데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명 액세스 시 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 ID 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS CLI 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
- 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결 AWS 될 때 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 API에서 역할 정보를 가져올 수 있습니다 AWS .

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지

를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포

함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔티티에 대한 권한 경계를 참조하세요.

- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 기업이 소유한 여러 AWS 계정 를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 참조하세요.
- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

AWS Config 에서 IAM을 사용하는 방법

IAM을 사용하여에 대한 액세스를 관리하기 전에 사용할 수 있는 IAM 기능에 대해 AWS Config알아봅니다 AWS Config.

에서 사용할 수 있는 IAM 기능 AWS Config

IAM 기능	AWS Config 지원
ID 기반 정책	예

IAM 기능	AWS Config 지원
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	예

AWS Config 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방법을 개괄적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

에 대한 자격 증명 기반 정책 AWS Config

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

에 대한 자격 증명 기반 정책 예제 AWS Config

자격 AWS Config 증명 기반 정책의 예를 보려면 섹션을 참조하세요에 대한 자격 증명 기반 정책 예제 AWS Config.

내의 리소스 기반 정책 AWS Config

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

에 대한 정책 작업 AWS Config

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

AWS Config 작업 목록을 보려면 서비스 승인 참조의에서 정의한 작업을 AWS Config 참조하세요.

의 정책 작업은 작업 앞에 다음 접두사를 AWS Config 사용합니다.

```
config
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "config:action1",
      "config:action2"
         ]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `Describe`라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "config:Describe*"
```

자격 AWS Config 증명 기반 정책의 예를 보려면 섹션을 참조하세요에 대한 자격 증명 기반 정책 예제 AWS Config.

에 대한 정책 리소스 AWS Config

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

AWS Config 리소스 유형 및 해당 ARNs 목록을 보려면 서비스 승인 참조의에서 정의한 리소스를 AWS Config 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Config가 정의한 작업을 참조하십시오.

자격 AWS Config 증명 기반 정책의 예를 보려면 섹션을 참조하세요에 대한 자격 증명 기반 정책 예제 AWS Config.

에 대한 정책 조건 키 AWS Config

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 `OR` 작업을 사용하여 조건을 AWS 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

AWS Config 조건 키 목록을 보려면 서비스 승인 참조의에 대한 조건 키를 AWS Config 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 에서 정의한 작업을 AWS Config 참조하세요.

자격 AWS Config 증명 기반 정책의 예를 보려면 섹션을 참조하세요에 대한 자격 증명 기반 정책 예제 AWS Config.

ACLs AWS Config

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 위탁자(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

를 사용한 ABAC AWS Config

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

AWS Config 리소스 태그 지정에 대한 자세한 내용은 섹션을 참조하세요AWS Config 리소스 태그 지정.

에서 임시 자격 증명 사용 AWS Config

임시 자격 증명 지원: 예

일부 AWS 서비스 는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 비롯한 추가 정보는 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는 섹션을 참조하세요.

사용자 이름과 암호를 제외한 방법을 AWS Management Console 사용하여에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 access AWS. AWS recommends에 액세스할 수 있습니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

에 대한 전달 액세스 세션 AWS Config

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AWS Config의 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.

> **Warning**
> 서비스 역할에 대한 권한을 변경하면 AWS Config 기능이 중단될 수 있습니다. 에서 관련 지침을 AWS Config 제공하는 경우에만 서비스 역할을 편집합니다.

에 대한 서비스 연결 역할 AWS Config

서비스 링크 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

AWS Config 서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 섹션을 참조하세요에 서비스 연결 역할 사용 AWS Config.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하세요. 서비스 연결 역할 열에서 `Yes`이(가) 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

에 대한 자격 증명 기반 정책 예제 AWS Config

기본적으로 사용자 및 역할에는 AWS Config 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하

여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARNs 형식을 포함하여 AWS Config에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 에 사용되는 작업, 리소스 및 조건 키를 AWS Config 참조하세요.

주제

- 정책 모범 사례
- 에 가입 AWS 계정
- 관리자 액세스 권한이 있는 사용자 생성
- AWS Config 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- 에 대한 읽기 전용 액세스 AWS Config
- 에 대한 전체 액세스 AWS Config
- AWS Config 규칙 API 작업에 지원되는 리소스 수준 권한
- 다중 계정 다중 리전 데이터 집계에 지원되는 리소스 수준 권한

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 AWS Config 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.

- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

에 가입 AWS 계정

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   가입 절차의 일부로는 전화 또는 문자 메시지를 수신하고 전화 키패드에 확인 코드를 입력하는 것이 포함됩니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 AWS 계정보호 AWS IAM Identity Center, AWS 계정 루트 사용자활성화 및 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자AWS Management Console로에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 자격 증명 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 사용 AWS IAM Identity Center 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.

2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

AWS Config 콘솔 사용

AWS Config 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은의 AWS Config 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 AWS Config 콘솔을 계속 사용할 수 있도록 하려면 관리형 AWS Config *AWSConfigUserAccess* AWS 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

사용자에게 상호 작용할 수 있는 권한을 부여해야 합니다 AWS Config. 에 대한 전체 액세스 권한이 필요한 사용자의 경우 관리형 정책에 대한 전체 액세스 AWS Config 권한을 AWS Config사용합니다.

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요:

- 의 사용자 및 그룹 AWS IAM Identity Center:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용 설명서의 권한 세트 생성의 지침을 따릅니다.
- 보안 인증 공급자를 통해 IAM에서 관리되는 사용자:

  ID 페더레이션을 위한 역할을 생성합니다. IAM 사용 설명서의 Create a role for a third-party identity provider (federation)의 지침을 따릅니다.
- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용 설명서에서 Create a role for an IAM user의 지침을 따릅니다.
  - (권장되지 않음)정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따르세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

에 대한 읽기 전용 액세스 AWS Config

다음 예제에서는에 읽기 전용 액세스 권한을 `AWSConfigUserAccess` 부여하는 AWS 관리형 정책을 보여줍니다 AWS Config.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

정책 설명에서 `Effect` 요소는 작업 허용 또는 거부 여부를 지정합니다. `Action` 요소는 사용자가 수행할 수 있도록 허용된 특정 작업을 나열합니다. `Resource` 요소는 사용자가 해당 작업을 수행할 수 있는 AWS 리소스를 나열합니다. AWS Config 작업에 대한 액세스를 제어하는 정책의 경우 `Resource` 요소는 항상 "모든 리소스"를 의미하는 와일드카드`*`인 로 설정됩니다.

서비스가 지원하는 API에 대한 `Action` 요소의 값입니다. 작업 앞에는 작업을 참조함을 `config:` 나타내는 AWS Config 작업이 옵니다. 다음 예제와 같이 `*` 요소에서 `Action` 와일드카드 문자를 사용할 수 있습니다.

- `"Action": ["config:*ConfigurationRecorder"]`

  이렇게 하면 "ConfigurationRecorder"(`StartConfigurationRecorder`, `StopConfigurationRecorder`)로 끝나는 모든 AWS Config 작업이 허용됩니다.
- `"Action": ["config:*"]`

이렇게 하면 모든 AWS Config 작업이 허용되지만 다른 AWS 서비스에 대한 작업은 허용되지 않습니다.

- `"Action": ["*"]`

  이렇게 하면 모든 AWS 작업이 허용됩니다. 이 권한은 계정의 AWS 관리자 역할을 하는 사용자에게 적합합니다.

읽기 전용 정책에서는 `StartConfigurationRecorder`, `StopConfigurationRecorder`, 및 `DeleteConfigurationRecorder`와 같은 작업에 대한 사용자 권한을 허용하지 않습니다. 이 정책이 적용된 사용자는 구성 레코더를 시작, 중지 또는 삭제할 수 없습니다. AWS Config 작업 목록은 AWS Config API 참조를 참조하세요.

에 대한 전체 액세스 AWS Config

다음 예제에서는에 대한 전체 액세스 권한을 부여하는 정책을 보여줍니다 AWS Config. 사용자에게 모든 AWS Config 작업을 수행할 수 있는 권한을 부여합니다. 또한 사용자가 Amazon S3 버킷에서 파일을 관리하고, 사용자가 연결되어 있는 계정에서 Amazon SNS 주제를 관리할 수 있도록 합니다.

> **Important**
>
> 이 정책은 광범위한 권한을 부여합니다. 전체 액세스 권한을 부여하기 전에 최소한의 권한 세트로 시작하여 필요에 따라 추가 권한을 부여하는 것이 좋습니다. 처음부터 권한을 많이 부여한 후 나중에 줄이는 방법보다 이 방법이 더 안전합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
}
```

AWS Config 규칙 API 작업에 지원되는 리소스 수준 권한

리소스 수준 권한은 사용자가 작업을 수행할 수 있는 리소스를 지정하는 기능을 말합니다.는 특정 AWS Config 규칙 API 작업에 대한 리소스 수준 권한을 AWS Config 지원합니다. 즉, 특정 AWS Config 규칙 작업의 경우 사용자가 해당 작업을 사용할 수 있는 조건을 제어할 수 있습니다. 이러한 조건은 충족되어야 하는 작업이거나 사용자가 사용하도록 허용된 특정 리소스일 수 있습니다.

다음 표에서는 현재 리소스 수준 권한을 지원하는 AWS Config 규칙 API 작업을 설명합니다. 또한 각 작업에 지원되는 리소스 및 해당 ARN도 설명합니다. ARN을 지정할 때, 예를 들어, 정확한 리소스 ID를 지정할 수 없거나 지정하길 원치 않는 경우에는 경로에 * 와일드카드를 사용할 수 있습니다.

> **Important**
>
> AWS Config 규칙 API 작업이이 표에 나열되지 않은 경우 리소스 수준 권한을 지원하지 않습니다. AWS Config 규칙 작업이 리소스 수준 권한을 지원하지 않는 경우 사용자에게 작업을 사용할 수 있는 권한을 부여할 수 있지만 정책 설명의 리소스 요소에 *를 지정해야 합니다.

API 작업	리소스
DeleteConfigRule	Config 규칙 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DeleteEvaluationResults	Config 규칙 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeComplianceByConfigRule	Config 규칙 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeConfigRuleEvaluationStatus	Config 규칙 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
GetComplianceDetailsByConfigRule	Config 규칙 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutConfigRule	Config 규칙

API 작업	리소스
	arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
StartConfigRulesEvaluation	Config 규칙 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutRemediationConfigurations	문제 해결 구성 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationConfigurations	문제 해결 구성 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DeleteRemediationConfiguration	문제 해결 구성 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
PutRemediationExceptions	문제 해결 구성 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationExceptions	문제 해결 구성 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

API 작업	리소스
DeleteRemediationExceptions	문제 해결 구성 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

예를 들어, 특정 사용자에게 특정 규칙에 대해 읽기 액세스를 허용하고 쓰기 액세스를 거부할 수 있습니다.

첫 번째 정책에서는 `DescribeConfigRuleEvaluationStatus` 지정된 AWS Config 규칙에서와 같은 규칙 읽기 작업을 허용합니다.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "config:StartConfigRulesEvaluation",
                    "config:DescribeComplianceByConfigRule",
                    "config:DescribeConfigRuleEvaluationStatus",
                    "config:GetComplianceDetailsByConfigRule"
                ],
                "Resource": [
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID",
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID"
                ]
            }
        ]
    }
```

두 번째 정책에서는 특정 AWS Config 규칙에 대한 규칙 쓰기 작업을 거부합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
```

```
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
               ],
            "Resource": "arn:aws:config:region:accountID:config-rule/config-rule-ID"
           }
      ]
   }
```

리소스 수준 권한을 사용하면 읽기 액세스를 허용하고 쓰기 액세스를 거부하여 AWS Config 규칙 API 작업에 대한 특정 작업을 수행할 수 있습니다.

다중 계정 다중 리전 데이터 집계에 지원되는 리소스 수준 권한

리소스 수준 권한을 사용하여 다중 계정 다중 리전 데이터 집계 시 특정 작업을 수행하는 사용자의 기능을 제어할 수 있습니다. 다음 AWS Config `Aggregator` APIs 지원합니다.

- BatchGetAggregateResourceConfig
- DeleteConfigurationAggregator
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSourcesStatus
- GetAggregateComplianceDetailsByConfigRule
- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResourceCounts
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfigurationAggregator
- SelectAggregateResourceConfig

예를 들어 두 개의 집계자 `AccessibleAggregator` 및 `InAccessibleAggregator`를 생성하고 `AccessibleAggregator`에 대한 액세스는 허용하지만 `InAccessibleAggregator`에 대한 액세스는 거부하는 IAM 정책을 추가하여 특정 사용자의 리소스 데이터 액세스를 제한할 수 있습니다.

AccessibleAggregator에 대한 IAM 정책

이 정책에서는 지정한 AWS Config Amazon 리소스 이름(ARN)에 지원되는 집계자 작업에 대한 액세스를 허용합니다. 이 예제에서 AWS Config ARN은 입니다`arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-mocpsqhs`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-mocpsqhs"
        }
    ]
}
```

InAccessibleAggregator에 대한 IAM 정책

이 정책에서는 지정한 AWS Config ARN에 지원되는 집계자 작업에 대한 액세스를 거부합니다. 이 예제에서 AWS Config ARN은 입니다`arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-pokxzldx`.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

개발자 그룹의 사용자가 지정된 AWS Config ARN에서 이러한 작업을 수행하려고 하면 해당 사용자에게 액세스 거부 예외가 발생합니다.

사용자 액세스 권한 확인

생성한 집계자를 표시하려면 다음 AWS CLI 명령을 실행합니다.

```
aws configservice describe-configuration-aggregators
```

명령이 성공적으로 완료되면 계정과 관련된 모든 집계자의 세부 정보를 볼 수 있습니다. 다음 예제에서는 `AccessibleAggregator` 및 `InAccessibleAggregator`입니다.

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
```

```
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

> **Note**
>
> `account-aggregation-sources`에, 데이터를 집계하려는 AWS 계정 ID의 쉼표로 구분된 목록을 입력합니다. 계정 ID를 대괄호로 묶고 반드시 따옴표를 이스케이프 처리해야 합니다 (예: `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"], \"AllAwsRegions\": true}]"`).

`InAccessibleAggregator` 또는 액세스를 거부하려는 집계자에 다음 IAM 정책을 연결합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

그런 다음 IAM 정책이 특정 집계자의 규칙에 대한 액세스를 제한하도록 작동하는지 확인할 수 있습니다.

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

이 명령은 액세스 거부 예외를 반환할 것입니다.

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

AWS 에 대한 관리형 정책 AWS Config

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSConfigServiceRolePolicy

AWS Config 는 라는 서비스 연결 역할을 AWSServiceRoleForConfig 사용하여 사용자를 대신하여 다른 AWS 서비스를 호출합니다. AWS Management Console 를 사용하여 설정하면 자체 AWS Identity and Access Management (IAM) 서비스 역할 대신 SLR을 사용하는 옵션을 AWS Config 선택하면 AWS Config이 AWS Config SLR이에 의해 자동으로 생성됩니다.

AWSServiceRoleForConfig SLR에는 관리형 정책 `AWSConfigServiceRolePolicy`가 포함되어 있습니다. 이 관리형 정책에는 AWS Config 리소스에 대한 읽기 전용 및 쓰기 전용 권한과가 AWS Config 지원하는 다른 서비스의 리소스에 대한 읽기 전용 권한이 포함되어 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 및 에 서비스 연결 역할 사용 AWS Config 섹션을 참조하세요.

정책 보기: AWSConfigServiceRolePolicy.

> **권장 사항: 서비스 연결 역할 사용**
>
> 특정 사용 사례가 없는 한 서비스 연결 역할을 사용하는 것이 좋습니다. 서비스 연결 역할은 AWS Config 을 예상대로 실행하는 데 필요한 모든 권한을 추가합니다. 서비스 연결 구성 레코더와 같은 일부 기능을 사용하려면 서비스 연결 역할을 사용해야 합니다.

AWS 관리형 정책: AWS_ConfigRole

AWS 리소스 구성을 기록하려면에 리소스에 대한 구성 세부 정보를 가져오는 IAM 권한이 AWS Config 필요합니다. AWS Config용 IAM 역할을 생성하려는 경우 관리형 정책 `AWS_ConfigRole`을 사용하여 IAM 역할에 연결할 수 있습니다.

이 IAM 정책은가 AWS 리소스 유형에 대한 지원을 AWS Config 추가할 때마다 업데이트됩니다. 즉, AWS_ConfigRole 역할에이 관리형 정책이 연결되어 있는 한는 지원되는 리소스 유형의 구성 데이터를 기록하는 데 필요한 권한을 계속 갖게 AWS Config 됩니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 및 에 할당된 IAM 역할에 대한 권한 AWS Config 섹션을 참조하세요.

정책 보기: AWS_ConfigRole.

AWS 관리형 정책: AWSConfigUserAccess

이 IAM 정책은 리소스의 태그별 검색 및 모든 태그 읽기 AWS Config를 포함하여 사용할 수 있는 액세스 권한을 제공합니다. 이는 관리 권한이 필요한를 구성할 수 AWS Config있는 권한을 제공하지 않습니다.

AWSConfigUserAccess 정책을 확인합니다.

AWS 관리형 정책: ConfigConformsServiceRolePolicy

적합성 팩을 배포하고 관리하려면 다른 AWS 서비스의 IAM 권한과 특정 권한이 AWS Config 필요합니다. 이를 통해 전체 기능을 갖춘 적합성 팩을 배포하고 관리할 수 있으며가 적합성 팩에 대한 새 기능을 AWS Config 추가할 때마다 업데이트됩니다. 적합성 팩에 대한 자세한 내용은 적합성 팩을 참조하세요.

정책 보기: ConfigConformsServiceRolePolicy.

AWS 관리형 정책: AWSConfigRulesExecutionRole

AWS 사용자 지정 Lambda 규칙을 배포하려면에 IAM 권한과 다른 AWS 서비스의 특정 권한이 AWS Config 필요합니다. 이를 통해 AWS Lambda 함수는 AWS Config API 및가 Amazon S3에 주기적으로 AWS Config 전송하는 구성 스냅샷에 액세스할 수 있습니다. 이 액세스는 AWS 사용자 지정 Lambda 규칙에 대한 구성 변경을 평가하는 함수에 필요하며가 새 기능을 AWS Config 추가할 때마다 업데이트됩니다. AWS 사용자 지정 Lambda 규칙에 대한 자세한 내용은 AWS Config 사용자 지정 Lambda 규칙 생성을 참조하세요. 구성 스냅샷에 대한 자세한 내용은 개념 | 구성 스냅샷을 참조하세요. 구성 스냅샷 전송에 대한 자세한 내용은 전송 채널 관리를 참조하세요.

정책 보기: AWSConfigRulesExecutionRole.

AWS 관리형 정책: AWSConfigMultiAccountSetupPolicy

의 조직 내 멤버 계정 간에 AWS Config 규칙 및 적합성 팩을 중앙에서 배포, 업데이트 및 삭제하려면 다른 AWS 서비스의 IAM 권한과 특정 권한이 AWS Organizations AWS Config 필요합니다. 이 관리형 정책은 AWS Config 가 다중 계정 설정을 위한 새로운 기능을 추가할 때마다 업데이트됩니다. 자세한 내용은 조직의 모든 계정에서 AWS Config 규칙 관리 및 조직의 모든 계정에서 적합성 팩 관리를 참조하세요.

정책 보기: AWSConfigMultiAccountSetupPolicy.

AWS 관리형 정책: AWSConfigRoleForOrganizations

가 읽기 전용 AWS Organizations APIs 호출 AWS Config 하도록 허용하려면 다른 AWS 서비스의 IAM 권한과 특정 권한이 AWS Config 필요합니다. 이 관리형 정책은 AWS Config 가 다중 계정 설정을 위한 새로운 기능을 추가할 때마다 업데이트됩니다. 자세한 내용은 조직의 모든 계정에서 AWS Config 규칙 관리 및 조직의 모든 계정에서 적합성 팩 관리를 참조하세요.

정책 보기: AWSConfigRoleForOrganizations.

AWS 관리형 정책: AWSConfigRemediationServiceRolePolicy

AWS Config 가 사용자를 대신하여 `NON_COMPLIANT` AWS Config 리소스를 수정할 수 있도록 하려면 에 IAM 권한과 다른 AWS 서비스의 특정 권한이 필요합니다. 이 관리형 정책은가 문제 해결을 위한 새 기능을 AWS Config 추가할 때마다 업데이트됩니다. 문제 해결에 대한 자세한 내용은 AWS Config 규칙을 사용하여 규정 미준수 리소스 문제 해결을 참조하세요. 가능한 AWS Config 평가 결과를 시작하는 조건에 대한 자세한 내용은 개념 | AWS Config 규칙을 참조하세요.

정책 보기: AWSConfigRemediationServiceRolePolicy.

AWS ConfigAWS 관리형 정책에 대한 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS Config 이후부터의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AWS Config 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AWS_ConfigRole – "bedrock: GetGuardrail", "bedrock: GetInferenceProfile", "bedr	이제이 정책은 Amazon Bedrock에 대한 추가 권한을 지원합니다.	2025년 5월 27일

변경 사항	설명	날짜
ock:GetKnowledgeBase", "bedrock:ListGuardrails", " bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource" 추가		
AWSConfigServiceRolePolicy – "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", " bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource" 추가	이제이 정책은 Amazon Bedrock에 대한 추가 권한을 지원합니다.	2025년 5월 27일

변경 사항	설명	날짜
AWS_ConfigRole – "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", "route53profi	이제이 정책은 Amazon Bedrock AWS B2B Data Interchange, AWS Clean Rooms, AWS CodeConnections AWS Direct Connect,, AWS Database Migration Service (AWS DMS), Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service(Amazon S3), Amazon SageMaker AI AWS Security Hub및 AWS Systems Manager Incident Manager연락처 AWS Systems Manager Incident Manager 에 대한 추가 권한을 지원합니다 AWS Systems Manager.	2025년 4월 8일

변경 사항	설명	날짜
les:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsFor Resource", "s3:GetAccessGra ntsInstance", "s3:GetAc cessGrantsLocation", "s3:Li stAccessGrantsInstances", "s3:ListAccessGrantsLocatio ns", "sagemaker:DescribeClu ster", "sagemaker:DescribeM lflowTrackingServer", "sage maker:DescribeStudioLifecyc leConfig", "sagemaker:ListC lusters", "sagemaker:ListMlf lowTrackingServers", "sagem aker:ListStudioLifecycleCon figs", "securityhub:Describ eStandardsControls", "secur ityhub:GetEnabledStandards" , "ssm-contacts:GetContact", "ssm-contacts:GetContactCha nnel", "ssm-contacts:ListCo ntactChannels", "ssm-cont acts:ListContacts", "ssm-in cidents:GetResponsePlan", " ssm-incidents:ListResponseP lans", "ssm-incidents:ListT agsForResource", "ssm:Descr ibeInstanceInformation" 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", "route53profi	이제이 정책은 Amazon Bedrock AWS B2B Data Interchange, AWS Clean Rooms, AWS CodeConnections AWS Direct Connect,, AWS Database Migration Service (AWS DMS), Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service(Amazon S3), Amazon SageMaker AI AWS Security Hub및 AWS Systems Manager Incident Manager연락처 AWS Systems Manager Incident Manager 에 대한 추가 권한을 지원합니다 AWS Systems Manager. 이 정책은 이제 리소스 패턴 `"arn:aws:apigateway:::/domainnames/ "`을 포함하여 모든 Amazon API Gateway 도메인 이름에 액세스할 수 있는 권한도 지원합니다.	2025년 4월 8일

변경 사항	설명	날짜
les:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsForResource", "s3:GetAccessGrantsInstance", "s3:GetAccessGrantsLocation", "s3:ListAccessGrantsInstances", "s3:ListAccessGrantsLocations", "sagemaker:DescribeCluster", "sagemaker:DescribeMlflowTrackingServer", "sagemaker:DescribeStudioLifecycleConfig", "sagemaker:ListClusters", "sagemaker:ListMlflowTrackingServers", "sagemaker:ListStudioLifecycleConfigs", "securityhub:DescribeStandardsControls", "securityhub:GetEnabledStandards", "ssm-contacts:GetContact", "ssm-contacts:GetContactChannel", "ssm-contacts:ListContactChannels", "ssm-contacts:ListContacts", "ssm-incidents:GetResponsePlan", "ssm-incidents:ListResponsePlans", "ssm-incidents:ListTagsForResource", "ssm:DescribeInstanceInformation" 추가		
AWS_ConfigRole – "ec2:GetAllowedImagesSettings" 추가	이제이 정책은 Amazon Elastic Compute Cloud(Amazon EC2)에 대한 추가 권한을 지원합니다.	2025년 3월 4일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – "ec2:GetAllowedImagesSettings" 추가	이제이 정책은 Amazon Elastic Compute Cloud(Amazon EC2)에 대한 추가 권한을 지원합니다.	2025년 3월 4일
AWS_ConfigRole – "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools" 추가	이제이 정책은 Amazon Comprehend AWS Clean Rooms, Amazon Elastic Compute Cloud(Amazon EC2), AWS HealthOmics Amazon Simple Storage Service(Amazon S3) 및 Amazon Simple Email Service(Amazon SES)에 대한 추가 권한을 지원합니다.	2025년 1월 16일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools" 추가	이제이 정책은 Amazon Comprehend AWS Clean Rooms, Amazon Elastic Compute Cloud(Amazon EC2), AWS HealthOmics Amazon Simple Storage Service(Amazon S3) 및 Amazon Simple Email Service(Amazon SES)에 대한 추가 권한을 지원합니다.	2025년 1월 16일
AWSConfigServiceRolePolicy – "organizations:ListAWSServiceAccessForOrganization" 추가	이 정책은 이제에 대한 추가 권한을 지원합니다 AWS Organizations.	2024년 12월 18일

변경 사항	설명	날짜
AWS_ConfigRole – "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType", "iot:ListThingGroups", "iot	이제이 정책은 AWS AppConfig, AWS CloudTrail Amazon Connect, Amazon DataZone, Amazon DevOpsGuru, AWS Glue, Identity Store, AWS IoT, AWS IoT FleetWise, AWS IoT 무선,, Amazon Interactive Video Service(Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager, AWS Payment Cryptography, Amazon Relational Database Service(Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service(Amazon S3), Amazon EventBridge Scheduler AWS Systems Manager및 Amazon VPC Lattice에 대한 추가 권한을 지원합니다.	2024년 11월 7일

변경 사항	설명	날짜
:ListThingTypes", "iotfleetwise:GetDecoderManifest", "iotfleetwise:GetFleet", "iotfleetwise:GetModelManifest", "iotfleetwise:GetSignalCatalog", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderManifestNetworkInterfaces", "iotfleetwise:ListDecoderManifests", "iotfleetwise:ListDecoderManifestSignals", "iotfleetwise:ListFleets", "iotfleetwise:ListModelManifestNodes", "iotfleetwise:ListModelManifests", "iotfleetwise:ListSignalCatalogNodes", "iotfleetwise:ListSignalCatalogs", "iotfleetwise:ListTagsForResource", "iotfleetwise:ListVehicles", "iotwireless:GetDestination", "iotwireless:GetDeviceProfile", "iotwireless:GetWirelessGateway", "iotwireless:ListDestinations", "iotwireless:ListDeviceProfiles", "iotwireless:ListWirelessGateways", "ivschat:GetLoggingConfiguration", "ivschat:GetRoom" "ivschat:ListLoggingConfigurations", "ivschat:ListRooms", "ivschat:ListTagsForResource", "logs:GetLogAnomalyDetector", "logs:ListLogAnomalyDetectors", "oam:GetS		

변경 사항	설명	날짜
ink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets" 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType", "iot:ListThingGroups", "iot	이제이 정책은 AWS AppConfig, AWS CloudTrail Amazon Connect, Amazon DataZone, Amazon DevOpsGuru, AWS Glue, Identity Store, AWS IoT, AWS IoT FleetWise, AWS IoT 무선,, Amazon Interactive Video Service(Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager, AWS Payment Cryptography, Amazon Relational Database Service(Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service(Amazon S3), Amazon EventBridge Scheduler AWS Systems Manager및 Amazon VPC Lattice에 대한 추가 권한을 지원합니다.	2024년 11월 7일

변경 사항	설명	날짜
:ListThingTypes", "iotfleetwise:GetDecoderManifest", "iotfleetwise:GetFleet", "iotfleetwise:GetModelManifest", "iotfleetwise:GetSignalCatalog", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderManifestNetworkInterfaces", "iotfleetwise:ListDecoderManifests", "iotfleetwise:ListDecoderManifestSignals", "iotfleetwise:ListFleets", "iotfleetwise:ListModelManifestNodes", "iotfleetwise:ListModelManifests", "iotfleetwise:ListSignalCatalogNodes", "iotfleetwise:ListSignalCatalogs", "iotfleetwise:ListTagsForResource", "iotfleetwise:ListVehicles", "iotwireless:GetDestination", "iotwireless:GetDeviceProfile", "iotwireless:GetWirelessGateway", "iotwireless:ListDestinations", "iotwireless:ListDeviceProfiles", "iotwireless:ListWirelessGateways", "ivschat:GetLoggingConfiguration", "ivschat:GetRoom" "ivschat:ListLoggingConfigurations", "ivschat:ListRooms", "ivschat:ListTagsForResource", "logs:GetLogAnomalyDetector", "logs:ListLogAnomalyDetectors", "oam:GetS		

변경 사항	설명	날짜
ink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets" 추가		

변경 사항	설명	날짜
AWS_ConfigRole – "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup," "iot:ListBillingGroups," "ivs:GetEncoderConfiguration," "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration," "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest	이제이 정책은 Amazon OpenSearch Service Severless, Amazon AppStream, AWS Backup, AWS CloudTrail AWS Glue,, EC2 Image Builder, AWS IoT Amazon Interactive Video Service(Amazon IVS), AWS Elemental MediaConnect, AWS Elemental MediaTail or AWS HealthOmics, 및 Amazon EventBridge 스케줄러에 대한 추가 권한을 지원합니다.	2024년 9월 16일

변경 사항	설명	날짜
rictionPolicies," "ivs:ListStages," "ivs:ListStorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules" 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup, " "iot:ListBillingGroups," "ivs:GetEncoderConfiguration, " "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration, " "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest	이제이 정책은 Amazon OpenSearch Service Severless, Amazon AppStream, AWS Backup, AWS CloudTrail AWS Glue,, EC2 Image Builder, AWS IoT Amazon Interactive Video Service(Amazon IVS), AWS Elemental MediaConnect, AWS Elemental MediaTailor AWS HealthOmics, 및 Amazon EventBridge 스케줄러에 대한 추가 권한을 지원합니다.	2024년 9월 16일

변경 사항	설명	날짜
rictionPolicies," "ivs:ListStages," "ivs:ListStorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules" 추가		
AWS_ConfigRole – "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource" 추가	이제이 정책은 Amazon Elastic File System(Amazon EFS), Amazon Redshift 및에 대한 추가 권한을 지원합니다 AWS Systems Manager for SAP.	2024년 6월 17일
AWSConfigServiceRolePolicy – "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource" 추가	이제이 정책은 Amazon Elastic File System(Amazon EFS), Amazon Redshift 및에 대한 추가 권한을 지원합니다 AWS Systems Manager for SAP.	2024년 6월 17일

변경 사항	설명	날짜
AWS_ConfigRole – "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:G	이제이 정책은 Amazon Managed Service for Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon ElastiCache, Amazon FSx, AWS Glue, AWS Identity and Access Management (IAM), AWS Lambda, AWS RAM, Amazon Redshift Serverless, Amazon SageMaker AI 및 Amazon Simple Notification Service(Amazon SNS)에 대한 추가 권한을 지원합니다.	2024년 2월 22일

변경 사항	설명	날짜
etSMSSandboxAccountStatus" 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and	이제이 정책은 Amazon Managed Service for Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon ElastiCache, Amazon FSx, AWS Glue, AWS Identity and Access Management (IAM), AWS Lambda, AWS RAM, Amazon Redshift Serverless, Amazon SageMaker AI 및 Amazon Simple Notification Service(Amazon SNS)에 대한 추가 권한을 지원합니다.	2024년 2월 22일

변경 사항	설명	날짜
"sns:GetSMSSandboxAccountStatus" 추가		
AWSConfigUserAccess - AWS Config 이 AWS 관리형 정책에 대한 변경 사항 추적 시작	이 정책은 리소스의 태그별 검색 및 모든 태그 읽기 AWS Config를 포함하여 사용할 수 있는 액세스 권한을 제공합니다. 이렇게 하면 관리 권한이 필요한를 구성할 수 AWS Config 있는 권한이 제공되지 않습니다.	2024년 2월 22일
AWS_ConfigRole – "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets" 추가	이제이 정책은 AWS AppConfig Amazon Managed Service for Prometheus, AWS Database Migration Service (AWS DMS), (AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon CloudWatch Logs AWS Organizations및 Amazon Simple Storage Service(Amazon S3)에 대한 추가 권한을 지원합니다.	2023년 12월 5일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets" 추가	이제이 정책은 AWS AppConfig Amazon Managed Service for Prometheus, AWS Database Migration Service (AWS DMS), (AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon CloudWatch Logs AWS Organizations및 Amazon Simple Storage Service(Amazon S3)에 대한 추가 권한을 지원합니다.	2023년 12월 5일

변경 사항	설명	날짜
AWS_ConfigRole – "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationAssociation	이 정책은 이제 Amazon Cognito, Amazon Connect, Amazon EMR, AWS Ground Station, AWS Mainframe Modernization, Amazon MemoryDB, AWS Organizations, Amazon QuickSight, Amazon Relational Database Service(RDS), Amazon Redshift, Amazon Route 53 AWS Service Catalog및에 대한 추가 권한을 지원합니다 AWS Transfer Family.	2023년 11월 17일

변경 사항	설명	날짜
s," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrL		

변경 사항	설명	날짜
ocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles" 추가		
AWS_ConfigRole – "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID" 추가	이 정책은 이제 `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` , `AWSConfigSLRApiGatewayStatementID` 에 대한 보안 식별자(SID)를 추가합니다.	2023년 11월 17일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect	이 정책은 이제 Amazon Cognito, Amazon Connect, Amazon EMR, AWS Ground Station, AWS Mainframe Modernization, Amazon MemoryDB, AWS Organizations, Amazon QuickSight, Amazon Relational Database Service(RDS), Amazon Redshift, Amazon Route 53 AWS Service Catalog및에 대한 추가 권한을 지원합니다 AWS Transfer Family.	2023년 11월 17일

변경 사항	설명	날짜
:ListIntegrationAssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCid		

변경 사항	설명	날짜
rBlocks," "route53:ListCidrLocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles" 추가		
AWSConfigServiceRolePolicy – "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID" 추가	이 정책은 이제 `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` , `AWSConfigSLRApiGatewayStatementID` 에 대한 보안 식별자(SID)를 추가합니다.	2023년 11월 17일

변경 사항	설명	날짜
AWS_ConfigRole – "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListT	이제이 정책은 AWS Private CA, AWS App Mesh Amazon Connect, Amazon Elastic Container Service(Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon GuardDuty, Amazon Inspector, AWS IoT AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka(Amazon MSK), AWS Lambda AWS Network Manager AWS Organizations, 및 Amazon SageMaker AI에 대한 추가 권한을 지원합니다.	2023년 10월 4일

변경 사항	설명	날짜
ags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob" 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListT	이제이 정책은 AWS Private CA, AWS App Mesh Amazon Connect, Amazon Elastic Container Service(Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon GuardDuty , Amazon Inspector, AWS IoT AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka(Amazon MSK), AWS Lambda AWS Network Manager AWS Organizations, 및 Amazon SageMaker AI에 대한 추가 권한을 지원합니다.	2023년 10월 4일

변경 사항	설명	날짜
ags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob" 추가		
AWSConfigServiceRolePolicy – "ssm:GetParameter" 제거	이제이 정책은 AWS Systems Manager (Systems Manager)에 대한 권한을 제거합니다.	2023년 9월 6일

변경 사항	설명	날짜
AWS_ConfigRole – "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSecrets", "macie2:ListTagsForR	이 정책은 이제 AWS App Mesh, AWS CloudFormation, Amazon CloudFront AWS CodeArtifact, AWS CodeBuild, Amazon Connect, AWS Glue, Amazon GuardDuty, AWS Identity and Access Management (IAM), Amazon Inspector, AWS IoT, AWS IoT TwinMaker, AWS IoT 무선, Amazon Managed Streaming for Apache Kafka, Amazon Macie, AWS Elemental MediaConnect, AWS Network Manager, AWS Organizations AWS 리소스 탐색기, Amazon Route 53, Amazon Simple Storage Service(Amazon S3) 및 Amazon Simple Notification Service(Amazon SNS)에 대한 추가 권한을 지원합니다.	2023년 7월 28일

변경 사항	설명	날짜
esource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy" 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	이제이 정책은 Amazon AppStream 2.0, AWS CloudFormation, Amazon CloudFront AWS App Mesh, AWS CodeArtifact, AWS CodeBuild, Amazon Connect, AWS Glue, Amazon GuardDuty, AWS Identity and Access Management (IAM), Amazon Inspector, AWS IoT AWS IoT TwinMaker, AWS IoT 무선, Amazon Managed Streaming for Apache Kafka, Amazon Macie, AWS Elemental MediaConnect, AWS Network Manager AWS Organizations,, AWS 리소스 탐색기, Amazon Route 53, Amazon Simple Storage Service(Amazon S3), Amazon Simple Notification Service(Amazon SNS) 및 Amazon EC2 Systems Manager(SSM)에 대한 추가 권한을 지원합니다.	2023년 7월 28일

변경 사항	설명	날짜
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource" 추가		

변경 사항	설명	날짜
AWS_ConfigRole – "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", “dynamodb:DescribeTableReplicaAutoScaling" "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	이 정책은 이제에 대한 추가 권한을 지원합니다 AWS Amplify. Amazon Connect AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena, AWS Batch, AWS CloudFormation, AWS CloudTrail, AWS CodeArtifact, Amazon CodeGuru AWS Directory Service, Amazon DynamoDB, Amazon Elastic Compute Cloud(Amazon EC2), Amazon CloudWatch Evidently, AWS Organizations, Amazon Forecast, AWS IoT Greengrass, AWS Ground Station, AWS Identity and Access Management (IAM), Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon Lightsail, Amazon CloudWatch Logs, AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud(Amazon VPC), Personalize, Amazon QuickSight AWS Migration Hub Refactor Spaces, Amazon Simple Storage Service(Amazon S3), Amazon SageMaker AI, AWS Transfer Family.	2023년 6월 13일

변경 사항	설명	날짜
tasetGroup", "forecast :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases" "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts",		

변경 사항	설명	날짜
"organizations:ListAccounts ForParent", "organizations:L istOrganizationalUnitsForPa rent", "organizations:ListTa gsForResource", "personal ize:DescribeDataset", "perso nalize:DescribeDatasetGroup", "personalize:DescribeSchema ", "personalize:DescribeSolu tion", "personalize:ListD atasetGroups", "personalize: ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForRe source", "quicksight:ListTe mplates", "refactor-spaces:G etEnvironment", "refactor -spaces:GetService", "refactor-spaces:ListAppl ications", "refactor-spaces: ListEnvironments", "refactor -spaces:ListServices", "s3:GetAccessPointPolic yStatusForObjectLambda", "sagemaker:DescribeDe viceFleet", "sagemake r:DescribeFeatureGroup", "sa gemaker:ListDeviceFleets", "sagemaker:ListFeatureGroup s", "sagemaker:ListModels", and "transfer:ListTags ForResource" 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDatasetGroup", "forecast	이 정책은 이제에 대한 추가 권한을 지원합니다 AWS Amplify. Amazon Connect AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena, AWS Batch, AWS CloudFormation, AWS CloudTrail, AWS CodeArtifact, Amazon CodeGuru AWS Directory Service, Amazon DynamoDB, Amazon Elastic Compute Cloud(Amazon EC2), Amazon CloudWatch Evidently, AWS Organizations,Amazon Forecast, AWS IoT Greengrass, AWS Ground Station, AWS Identity and Access Management (IAM), Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon Lightsail, Amazon CloudWatch Logs, AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud(Amazon VPC), Personalize, Amazon QuickSight AWS Migration Hub Refactor Spaces, Amazon Simple Storage Service(Amazon S3), Amazon SageMaker AI, AWS Transfer Family.	2023년 6월 13일

변경 사항	설명	날짜
:ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "organizations:ListAccounts		

변경 사항	설명	날짜
ForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource" 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie2:GetClassificatio	이제이 정책은 Amazon Managed Workflows for AWS Amplify, AWS App Mesh AWS App Runner,,, Amazon CloudFront, AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, AWS Transfer Family, Amazon Pinpoint, AWS Migration Hub, AWS Resilience Hub, Amazon CloudWatch, AWS Directory Service 및에 대한 추가 권한을 지원합니다 AWS WAF.	2023년 4월 13일

변경 사항	설명	날짜
nExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations 추가		

변경 사항	설명	날짜
AWS_ConfigRole – amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie2:GetClassificatio	이제이 정책은 Amazon Managed Workflows for AWS Amplify, AWS App Mesh AWS App Runner,,, Amazon CloudFront, AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, AWS Transfer Family, Amazon Pinpoint, AWS Migration Hub, AWS Resilience Hub, Amazon CloudWatch, AWS Directory Service 및에 대한 추가 권한을 지원합니다 AWS WAF.	2023년 4월 13일

변경 사항	설명	날짜
nExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudfront:GetResponseHeadersPolicy, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstancePro	이제이 정책은 Amazon AppFlow, AWS App Runner, Amazon AppStream 2.0, Amazon CloudFront, Amazon CloudWatch, AWS CodeArtifact, AWS CodeCommit AWS Device Farm,, Amazon CloudWatch Evidently, Amazon Forecast, AWS Ground Station, AWS Identity and Access Management (IAM), AWS IoT, Amazon MemoryDB, Amazon Pinpoint, AWS Network Manager, AWS Panorama, Amazon Relational Database Service(RDS), Amazon Redshift 및 Amazon SageMaker AI에 대한 추가 권한을 지원합니다.	2023년 3월 30일

변경 사항	설명	날짜
file, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions 추가		

변경 사항	설명	날짜
AWS_ConfigRole – appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig,	이제이 정책은 Amazon Managed Workflows for Amazon AppFlow, AWS App Runner, Amazon AppStream 2.0, AWS CloudFormation, Amazon CloudFront, Amazon CloudWatch, AWS CodeArtifact, AWS CodeCommit AWS Device Farm, Amazon Elastic Compute Cloud(Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast AWS Ground Station, AWS Identity and Access Management (IAM), AWS IoT, Amazon MemoryDB, Amazon Pinpoint, AWS Network Manager AWS Panorama,, Amazon Relational Database Service(Amazon RDS), Amazon Redshift 및 Amazon SageMaker AI에 대한 추가 권한을 지원합니다.	2023년 3월 30일

변경 사항	설명	날짜
groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions 추가		

변경 사항	설명	날짜
AWSConfigRulesExecutionRole -이 AWS 관리형 정책에 대한 변경 사항 추적 AWS Config 시작	이 정책은 AWS Lambda 함수가 AWS Config API 및가 Amazon S3에 주기적으로 AWS Config 전송하는 구성 스냅샷에 액세스할 수 있도록 허용합니다. 이 액세스는 AWS 사용자 지정 Lambda 규칙에 대한 구성 변경을 평가하는 함수에 필요합니다.	2023년 3월 7일
AWSConfigRoleForOrganizations -이 AWS 관리형 정책에 대한 변경 사항 추적을 AWS Config 시작합니다.	이 정책은가 읽기 전용 AWS Organizations APIs 호출 AWS Config 하도록 허용합니다.	2023년 3월 7일
AWSConfigRemediationServiceRolePolicy -이 AWS 관리형 정책에 대한 변경 사항 추적을 AWS Config 시작합니다.	이 정책은 AWS Config 가 사용자를 대신하여 `NON_COMPLIANT` 리소스를 수정할 수 있도록 허용합니다.	2023년 3월 7일
AWSConfigServiceRolePolicy – auditmanager:GetAccountStatus 추가	이 정책은 이제 AWS Audit Manager내 계정의 등록 상태를 반환할 수 있는 권한을 부여합니다.	2023년 3월 3일
AWS_ConfigRole – auditmanager:GetAccountStatus 추가	이 정책은 이제 AWS Audit Manager내 계정의 등록 상태를 반환할 수 있는 권한을 부여합니다.	2023년 3월 3일

변경 사항	설명	날짜
AWSConfigMultiAccountSetupPolicy -이 AWS 관리형 정책에 대한 변경 사항 추적을 AWS Config 시작합니다.	이 정책은 AWS Config 가 AWS 서비스를 호출하고를 사용하여 조직 전체에 리소스를 배포할 AWS Config 수 있도록 허용합니다 AWS Organizations.	2023년 2월 27일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	이제이 정책은 Amazon Managed Workflows for Apache Airflow, AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer, AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller(ARC), AWS Device Farm, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Pinpoint, AWS Identity and Access Management (IAM), Amazon GuardDuty 및 Amazon CloudWatch Logs에 대한 추가 권한을 지원합니다.	2023년 2월 1일

변경 사항	설명	날짜
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries 추가		

변경 사항	설명	날짜
AWS_ConfigRole – airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	이제이 정책은 Amazon Managed Workflows for Apache Airflow, AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer, AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller(ARC), AWS Device Farm, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Pinpoint, AWS Identity and Access Management (IAM), Amazon GuardDuty 및 Amazon CloudWatch Logs에 대한 추가 권한을 지원합니다.	2023년 2월 1일

변경 사항	설명	날짜
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries 추가		
ConfigConformsServiceRolePolicy – config:DescribeConfigRules 업데이트	보안 모범 사례로서 이 정책은 이제 `config:DescribeConfigRules` 에 대한 광범위한 리소스 수준 권한을 제거합니다.	2023년 1월 12일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	이제이 정책은 Amazon Managed Service for Prometheus, AWS Audit Manager, AWS Device Farm, AWS Database Migration Service (AWS DMS), AWS Directory Service Amazon Elastic Compute Cloud(Amazon EC2), AWS Glue, AWS IoT, Amazon Lightsail, AWS Elemental MediaPackage, AWS Network Manager, Amazon QuickSight, AWS Resource Access Manager Amazon Application Recovery Controller(ARC), Amazon Simple Storage Service(Amazon S3) 및 Amazon Timestream에 대한 추가 권한을 지원합니다.	2022년 12월 15일

변경 사항	설명	날짜
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource 추가		

변경 사항	설명	날짜
AWS_ConfigRole – APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsForResource, quicksight:D	이제이 정책은 Amazon Managed Service for Prometheus, AWS Audit Manager, AWS Device Farm, AWS Database Migration Service (AWS DMS), AWS Directory Service Amazon Elastic Compute Cloud(Amazon EC2), AWS Glue, AWS IoT, Amazon Lightsail, AWS Elemental MediaPackage, AWS Network Manager, Amazon QuickSight, AWS Resource Access Manager Amazon Application Recovery Controller(ARC), Amazon Simple Storage Service(Amazon S3) 및 Amazon Timestream에 대한 추가 권한을 지원합니다.	2022년 12월 15일

변경 사항	설명	날짜
escribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – cloudformation:ListStackResources and cloudformation:ListStacks 추가	이제이 정책은 지정된 AWS CloudFormation 스택의 모든 리소스에 대한 설명을 반환하고 상태가 지정된와 일치하는 스택에 대한 요약 정보를 반환할 수 있는 권한을 부여합니다 StackStatusFilter.	2022년 11월 7일
AWS_ConfigRole – cloudformation:ListStackResources and cloudformation:ListStacks 추가	이제이 정책은 지정된 AWS CloudFormation 스택의 모든 리소스에 대한 설명을 반환하고 상태가 지정된와 일치하는 스택에 대한 요약 정보를 반환할 수 있는 권한을 부여합니다 StackStatusFilter.	2022년 11월 7일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	이 정책은 이제에 대한 추가 권한을 지원합니다 AWS Certificate Manager. Amazon Managed Workflows for Apache Airflow, AWS Amplify, AWS AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect AWS Glue DataBrew, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Elastic Kubernetes Service(Amazon EKS), Amazon EventBridge, AWS Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift 서버, Amazon Location Service AWS IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, AWS OpsWorks, AWS Panorama, AWS Resource Access Manager, Amazon QuickSight, Amazon Relational Database Service(RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service(Amazon S3), AWS Cloud Map, 및 AWS Security Token Service.	2022년 10월 19일

변경 사항	설명	날짜
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

변경 사항	설명	날짜
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

변경 사항	설명	날짜
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups 추가		

변경 사항	설명	날짜
AWS_ConfigRole – acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	이 정책은 이제에 대한 추가 권한을 지원합니다 AWS Certificate Manager. Amazon Managed Workflows for Apache Airflow, AWS Amplify, AWS AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect AWS Glue DataBrew, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Elastic Kubernetes Service(Amazon EKS), Amazon EventBridge, AWS Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift 서버, Amazon Location Service AWS IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, AWS OpsWorks, AWS Panorama, AWS Resource Access Manager, Amazon QuickSight, Amazon Relational Database Service(RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service(Amazon S3), AWS Cloud Map, 및 AWS Security Token Service.	2022년 10월 19일

변경 사항	설명	날짜
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

변경 사항	설명	날짜
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

변경 사항	설명	날짜
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – Glue::GetTable 추가	이제이 정책은 지정된 AWS Glue 테이블의 데이터 카탈로그에서 테이블 정의를 검색할 수 있는 권한을 부여합니다.	2022년 9월 14일
AWS_ConfigRole – Glue::GetTable 추가	이제이 정책은 지정된 AWS Glue 테이블의 데이터 카탈로그에서 테이블 정의를 검색할 수 있는 권한을 부여합니다.	2022년 9월 14일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	이 정책은 이제 Amazon AppFlow에 대한 추가 권한을 지원합니다. Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOpsGuru, Amazon Elastic Compute Cloud(Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge 스키마, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift 서버, Amazon Interactive Video Service(Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller(ARC), Amazon Route 53 Resolver, Amazon Simple Storage	2022년 9월 7일

변경 사항	설명	날짜
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	Service(Amazon S3), Amazon SimpleDB Amazon Simple Email Service(Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync AWS Auto Scaling, AWS Backup,, AWS Budgets, AWS Cost Explorer, AWS Cloud9 AWS Directory Service, AWS DataSync,,, AWS Elemental MediaPackage AWS Glue, AWS IoT, AWS IoT Analytics, AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker,, AWS Lake Formation AWS License Manager,, AWS Resilience Hub AWS Signer, 및 AWS Transfer Family.	

변경 사항	설명	날짜
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

변경 사항	설명	날짜
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

변경 사항	설명	날짜
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

변경 사항	설명	날짜
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

변경 사항	설명	날짜
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

변경 사항	설명	날짜
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

변경 사항	설명	날짜
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

변경 사항	설명	날짜
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource 추가		

변경 사항	설명	날짜
AWS_ConfigRole – appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	이 정책은 이제 Amazon AppFlow에 대한 추가 권한을 지원합니다. Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOpsGuru, Amazon Elastic Compute Cloud(Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge 스키마, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift 서버, Amazon Interactive Video Service(Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller(ARC), Amazon Route 53 Resolver, Amazon Simple Storage	2022년 9월 7일

변경 사항	설명	날짜
ts, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	Service(Amazon S3), Amazon SimpleDB Amazon Simple Email Service(Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync AWS Auto Scaling, AWS Backup,, AWS Budgets, AWS Cost Explorer, AWS Cloud9 AWS Directory Service, AWS DataSync,,, AWS Elemental MediaPackage AWS Glue, AWS IoT, AWS IoT Analytics, AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker,, AWS Lake Formation AWS License Manager,, AWS Resilience Hub AWS Signer, 및 AWS Transfer Family	

변경 사항	설명	날짜
ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

변경 사항	설명	날짜
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

변경 사항	설명	날짜
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

변경 사항	설명	날짜
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

변경 사항	설명	날짜
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

변경 사항	설명	날짜
olicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

변경 사항	설명	날짜
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

변경 사항	설명	날짜
ansfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefarm:ListTestGridProj	이제이 정책은 Amazon Managed Workflows for Apache Airflow, AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller(ARC), AWS Device Farm Amazon Elastic Compute Cloud(Amazon EC2), Amazon Pinpoint, AWS Identity and Access Management (IAM), Amazon GuardDuty 및 Amazon CloudWatch Logs에 대한 추가 권한을 지원합니다.	2023년 2월 1일

변경 사항	설명	날짜
ects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries 추가		

변경 사항	설명	날짜
AWS_ConfigRole – airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	이제이 정책은 Amazon Managed Workflows for Apache Airflow, AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer, AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller(ARC), AWS Device Farm, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Pinpoint, AWS Identity and Access Management (IAM), Amazon GuardDuty 및 Amazon CloudWatch Logs에 대한 추가 권한을 지원합니다.	2023년 2월 1일

변경 사항	설명	날짜
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries 추가		
ConfigConformsServiceRolePolicy – config:DescribeConfigRules 업데이트	보안 모범 사례로서 이 정책은 이제 `config:DescribeConfigRules` 에 대한 광범위한 리소스 수준 권한을 제거합니다.	2023년 1월 12일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	이제이 정책은 Amazon Managed Service for Prometheus, AWS Audit Manager, AWS Device Farm, AWS Database Migration Service (AWS DMS), AWS Directory Service Amazon Elastic Compute Cloud(Amazon EC2), AWS Glue, AWS IoT, Amazon Lightsail, AWS Elemental MediaPackage, AWS Network Manager, Amazon QuickSight, AWS Resource Access Manager Amazon Application Recovery Controller(ARC), Amazon Simple Storage Service(Amazon S3) 및 Amazon Timestream에 대한 추가 권한을 지원합니다.	2022년 12월 15일

변경 사항	설명	날짜
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource 추가		

변경 사항	설명	날짜
AWS_ConfigRole – APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsForResource, quicksight:D	이제이 정책은 Amazon Managed Service for Prometheus, AWS Audit Manager, AWS Device Farm, AWS Database Migration Service (AWS DMS), AWS Directory Service Amazon Elastic Compute Cloud(Amazon EC2), AWS Glue, AWS IoT, Amazon Lightsail, AWS Elemental MediaPackage, AWS Network Manager, Amazon QuickSight, AWS Resource Access Manager Amazon Application Recovery Controller(ARC), Amazon Simple Storage Service(Amazon S3) 및 Amazon Timestream에 대한 추가 권한을 지원합니다.	2022년 12월 15일

변경 사항	설명	날짜
escribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – cloudformation:ListStackResources and cloudformation:ListStacks 추가	이제이 정책은 지정된 AWS CloudFormation 스택의 모든 리소스에 대한 설명을 반환하고 상태가 지정된와 일치하는 스택에 대한 요약 정보를 반환할 수 있는 권한을 부여합니다 StackStatusFilter.	2022년 11월 7일
AWS_ConfigRole – cloudformation:ListStackResources and cloudformation:ListStacks 추가	이제이 정책은 지정된 AWS CloudFormation 스택의 모든 리소스에 대한 설명을 반환하고 상태가 지정된와 일치하는 스택에 대한 요약 정보를 반환할 수 있는 권한을 부여합니다 StackStatusFilter.	2022년 11월 7일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	이 정책은 이제에 대한 추가 권한을 지원합니다 AWS Certificate Manager. Amazon Managed Workflows for Apache Airflow, AWS Amplify, AWS AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect AWS Glue DataBrew, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Elastic Kubernetes Service(Amazon EKS), Amazon EventBridge, AWS Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift 서버, Amazon Location Service AWS IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, AWS OpsWorks, AWS Panorama, AWS Resource Access Manager, Amazon QuickSight, Amazon Relational Database Service(RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service(Amazon S3), AWS Cloud Map, 및 AWS Security Token Service.	2022년 10월 19일

변경 사항	설명	날짜
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

변경 사항	설명	날짜
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

변경 사항	설명	날짜
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups 추가		

변경 사항	설명	날짜
AWS_ConfigRole – acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	이 정책은 이제에 대한 추가 권한을 지원합니다 AWS Certificate Manager. Amazon Managed Workflows for Apache Airflow, AWS Amplify, AWS AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect AWS Glue DataBrew, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Elastic Kubernetes Service(Amazon EKS), Amazon EventBridge, AWS Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift 서버, Amazon Location Service AWS IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, AWS OpsWorks, AWS Panorama, AWS Resource Access Manager, Amazon QuickSight, Amazon Relational Database Service(RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service(Amazon S3), AWS Cloud Map, 및 AWS Security Token Service.	2022년 10월 19일

변경 사항	설명	날짜
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

변경 사항	설명	날짜
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

변경 사항	설명	날짜
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – Glue::GetTable 추가	이제이 정책은 지정된 AWS Glue 테이블의 데이터 카탈로그에서 테이블 정의를 검색할 수 있는 권한을 부여합니다.	2022년 9월 14일
AWS_ConfigRole – Glue::GetTable 추가	이제이 정책은 지정된 AWS Glue 테이블의 데이터 카탈로그에서 테이블 정의를 검색할 수 있는 권한을 부여합니다.	2022년 9월 14일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	이 정책은 이제 Amazon AppFlow에 대한 추가 권한을 지원합니다. Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOpsGuru, Amazon Elastic Compute Cloud(Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge 스키마, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift 서버, Amazon Interactive Video Service(Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller(ARC), Amazon Route 53 Resolver, Amazon Simple Storage	2022년 9월 7일

변경 사항	설명	날짜
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	Service(Amazon S3), Amazon SimpleDB Amazon Simple Email Service(Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync AWS Auto Scaling, AWS Backup,, AWS Budgets, AWS Cost Explorer, AWS Cloud9 AWS Directory Service, AWS DataSync,,, AWS Elemental MediaPackage AWS Glue, AWS IoT, AWS IoT Analytics, AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker,, AWS Lake Formation AWS License Manager,, AWS Resilience Hub AWS Signer, 및 AWS Transfer Family.	

변경 사항	설명	날짜
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

변경 사항	설명	날짜
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

변경 사항	설명	날짜
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

변경 사항	설명	날짜
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

변경 사항	설명	날짜
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

변경 사항	설명	날짜
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

변경 사항	설명	날짜
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

변경 사항	설명	날짜
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource 추가		

변경 사항	설명	날짜
AWS_ConfigRole – appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	이 정책은 이제 Amazon AppFlow에 대한 추가 권한을 지원합니다. Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOpsGuru, Amazon Elastic Compute Cloud(Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge 스키마, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift 서버, Amazon Interactive Video Service(Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller(ARC), Amazon Route 53 Resolver, Amazon Simple Storage	2022년 9월 7일

변경 사항	설명	날짜
ts, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	Service(Amazon S3), Amazon SimpleDB Amazon Simple Email Service(Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync AWS Auto Scaling, AWS Backup,, AWS Budgets, AWS Cost Explorer, AWS Cloud9 AWS Directory Service, AWS DataSync,,, AWS Elemental MediaPackage AWS Glue, AWS IoT, AWS IoT Analytics, AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker,, AWS Lake Formation AWS License Manager,, AWS Resilience Hub AWS Signer, 및 AWS Transfer Family	

변경 사항	설명	날짜
ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

변경 사항	설명	날짜
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

변경 사항	설명	날짜
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

변경 사항	설명	날짜
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

변경 사항	설명	날짜
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

변경 사항	설명	날짜
olicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

변경 사항	설명	날짜
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

변경 사항	설명	날짜
ansfer:DescribeUser, transfer: DescribeWorkflow, transfer: ListServers, transfer:ListUsers , transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource 추가		
AWSConfigServiceRolePolicy – datasync:ListAgents, datasync:ListLocations, dat async:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists 추가	이제이 정책은에서 에이전트, DataSync 소스 및 대상 위치, DataSync 작업 목록을 AWS DataSync 반환하고 AWS 계정,에서 하나 이상의 지정된 네임스페이스와 연결된 네임스페이스 및 서비스에 대한 AWS Cloud Map 요약 정보를 나열하고 AWS 계정,에서 사용할 수 있는 모든 Amazon Simple Email Service(Amazon SES) 연락처 목록을 나열할 수 있는 권한을 부여합니다 AWS 계정.	2022년 8월 22일
AWS_ConfigRole – datasync: ListAgents, datasync:ListLocat ions, datasync:ListTasks, servicediscovery:ListNamesp aces, servicediscovery:List Services, and ses:ListContact Lists 추가	이제이 정책은에서 에이전트, DataSync 소스 및 대상 위치, DataSync 작업 목록을 AWS DataSync 반환하고 AWS 계정,에서 하나 이상의 지정된 네임스페이스와 연결된 네임스페이스 및 서비스에 대한 AWS Cloud Map 요약 정보를 나열하고 AWS 계정,에서 사용할 수 있는 모든 Amazon Simple Email Service(Amazon SES) 연락처 목록을 나열할 수 있는 권한을 부여합니다 AWS 계정.	2022년 8월 22일

변경 사항	설명	날짜
ConfigConformsServiceRolePolicy – cloudwatch:PutMetricData 추가	이 정책은 이제 Amazon CloudWatch에 지표 데이터 포인트를 게시할 수 있는 권한을 부여합니다.	2022년 7월 25일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De	이제이 정책은 Amazon Elastic Container Service(Amazon ECS), Amazon ElastiCache, Amazon EventBridge, Amazon FSx, Amazon Managed Service for Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon QuickSight, Amazon Rekognition AWS RoboMaker, Amazon Simple Storage Service(Amazon S3), Amazon Simple Email Service(Amazon SES), AWS Amplify, AWS AppConfig ,, AWS AppSync, AWS Billing Conductor, AWS Firewall Manager AWS DataSync, AWS Glue AWS IAM Identity Center ,(IAM Identity Center), EC2 Image Builder 및 Elastic Load Balancing에 대한 추가 권한을 지원합니다.	2022년 7월 15일

변경 사항	설명	날짜
scribeLocationS3, datasync: DescribeLocationSmb, datasy nc:DescribeTask, datasync: ListTagsForResource, ecr:De scribePullThroughCacheRules , ecr:DescribeRegistry, ecr:G etRegistryPolicy, elasticac he:DescribeCacheParameters, elasticloadbalancing:Descr ibeListenerCertificates, el asticloadbalancing:Describe TargetGroupAttributes, elas ticloadbalancing:DescribeTa rgetGroups, elasticloadbala ncing:DescribeTargetHealth, events:DescribeApiDestinat ion, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListP olicies, fms:ListTagsForRes ource, fsx:DescribeVolumes, geo:DescribeGeofenceColl ection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator , geo:DescribeTracker, geo:ListTrackerConsumers, g lue:BatchGetJobs, glue:Batc hGetWorkflows, glue:GetC rawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuil der: GetComponent, imagebuil der: ListComponentBuildVers ions, imagebuilder: ListCompo		

변경 사항	설명	날짜
nents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

변경 사항	설명	날짜
sso:GetInlinePolicyForPermissionSet 추가		

변경 사항	설명	날짜
AWS_ConfigRole – amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De	이제이 정책은 Amazon Elastic Container Service(Amazon ECS), Amazon ElastiCache, Amazon EventBridge, Amazon FSx, Amazon Managed Service for Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon QuickSight, Amazon Rekognition AWS RoboMaker, Amazon Simple Storage Service(Amazon S3), Amazon Simple Email Service(Amazon SES), AWS Amplify, AWS AppConfig ,, AWS AppSync, AWS Billing Conductor, AWS Firewall Manager AWS DataSync, AWS Glue AWS IAM Identity Center ,(IAM Identity Center), EC2 Image Builder 및 Elastic Load Balancing에 대한 추가 권한을 지원합니다.	2022년 7월 15일

변경 사항	설명	날짜
scribeLocationS3, datasync: DescribeLocationSmb, datasync:DescribeTask, datasync: ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVersions, imagebuilder: ListCompo		

변경 사항	설명	날짜
nents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

변경 사항	설명	날짜
sso:GetInlinePolicyForPermissionSet 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	이제이 정책은 지정된 Amazon Athena 데이터 카탈로그를 가져올 수 있는 권한을 부여합니다. 에 Athena 데이터 카탈로그 나열 AWS 계정및 Athena 작업 그룹 또는 데이터 카탈로그 리소스와 연결된 태그 나열 Amazon Detective 동작 그래프 목록을 가져오고 Detective 동작 그래프의 태그를 나열하려면 지정된 AWS Glue 개발 엔드포인트 이름 목록에 대한 리소스 메타데이터 목록 가져오기 지정된 AWS Glue 개발 엔드포인트에 대한 정보 가져오기 에서 AWS Glue 모든 개발 엔드포인트 가져오기 AWS 계정지정된 AWS Glue 보안 구성을 검색합니다. 모든 AWS Glue 보안 구성 가져오기 AWS Glue 리소스와 연결된 태그 목록 가져오기 지정된 이름의 AWS Glue 작업 그룹에 대한 정보 가져오기 계정에 있는 모든 AWS Glue 크롤러 리소스의 이름을 검색합니다. AWS 에 있는 모든 AWS Glue `DevEndpoint` 리소스의 이름을 가져옵니다 AWS 계정. 에 있는 모든 AWS Glue 작업 리소스의 이름을 나열합니다 AWS 계정. AWS Glue 멤버 계정에 대한 세부 정보 가져오기 계정에서 생성된 AWS Glue 워	2022년 5월 31일

변경 사항	설명	날짜
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource 추가	크플로의 목록 이름 및 계정에 사용 가능한 AWS Glue 작업 그룹 나열 Amazon GuardDuty 필터에 대한 세부 정보를 검색하려면 GuardDuty IPSet 검색 GuardDuty ThreatIntelSet 검색 GuardDuty 멤버 계정 검색 GuardDuty 필터 목록 가져오기 GuardDuty 서비스의 IPSets를 가져옵니다. GuardDuty Service에 대한 태그 검색 및 GuardDuty 서비스의 ThreatIntelSets 가져오기 Amazon Macie 계정의 현재 상태 및 구성 설정을 가져오는 방법 AWS Resource Access Manager (AWS RAM) 리소스 공유에 대한 리소스 및 보안 주체 연결을 검색하고 리소스 공유에 대한 AWS RAM 세부 정보를 검색합니다. Amazon Simple Email Service(Amazon SES) 기존 구성 세트에 대한 정보를 가져오려면 Amazon SES 구성 세트와 연결된 이벤트 대상 목록 가져오기 및 는 Amazon SES 계정과 연결된 모든 구성 세트를 나열합니다. Identity Center 디렉터리 속성 목록을 가져오려면 AWS IAM Identity Center 권한 세트의 세부 정보를 가져옵니다. 지정된 IAM Identity Center 권한 세트에 연결된 IAM 관리형 정책을 가져옵니다. IAM Identity	

변경 사항	설명	날짜
	Center 인스턴스에 대해 설정된 권한 가져오기 및 IAM Identity Center 리소스에 대한 태그를 가져옵니다.	

변경 사항	설명	날짜
AWS_ConfigRole – athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	이제이 정책은 지정된 Amazon Athena 데이터 카탈로그를 가져올 수 있는 권한을 부여합니다. 에 Athena 데이터 카탈로그 나열 AWS 계정및 Athena 작업 그룹 또는 데이터 카탈로그 리소스와 연결된 태그 나열 Amazon Detective 동작 그래프 목록을 가져오고 Detective 동작 그래프의 태그를 나열하려면 지정된 AWS Glue 개발 엔드포인트 이름 목록에 대한 리소스 메타데이터 목록 가져오기 지정된 AWS Glue 개발 엔드포인트에 대한 정보 가져오기 에서 AWS Glue 모든 개발 엔드포인트 가져오기 AWS 계정지정된 AWS Glue 보안 구성을 검색합니다. 모든 AWS Glue 보안 구성 가져오기 AWS Glue 리소스와 연결된 태그 목록 가져오기 지정된 이름의 AWS Glue 작업 그룹에 대한 정보 가져오기 계정에 있는 모든 AWS Glue 크롤러 리소스의 이름을 검색합니다. AWS 에 있는 모든 AWS Glue `DevEndpoint` 리소스의 이름을 가져옵니다 AWS 계정. 에 있는 모든 AWS Glue 작업 리소스의 이름을 나열합니다 AWS 계정. AWS Glue 멤버 계정에 대한 세부 정보 가져오기 계정에서 생성된 AWS Glue 워	2022년 5월 31일

변경 사항	설명	날짜
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource 추가	크플로의 목록 이름 및 계정에 사용 가능한 AWS Glue 작업 그룹 나열 Amazon GuardDuty 필터에 대한 세부 정보를 검색하려면 GuardDuty IPSet 검색 GuardDuty ThreatIntelSet 검색 GuardDuty 멤버 계정 검색 GuardDuty 필터 목록 가져오기 GuardDuty 서비스의 IPSets를 가져옵니다. GuardDuty Service에 대한 태그 검색 및 GuardDuty 서비스의 ThreatIntelSets 가져오기 Amazon Macie 계정의 현재 상태 및 구성 설정을 가져오는 방법 AWS Resource Access Manager (AWS RAM) 리소스 공유에 대한 리소스 및 보안 주체 연결을 검색하고 리소스 공유에 대한 AWS RAM 세부 정보를 검색합니다. Amazon Simple Email Service(Amazon SES) 기존 구성 세트에 대한 정보를 가져오려면 Amazon SES 구성 세트와 연결된 이벤트 대상 목록 가져오기 및 는 Amazon SES 계정과 연결된 모든 구성 세트를 나열합니다. Identity Center 디렉터리 속성 목록을 가져오려면 AWS IAM Identity Center 권한 세트의 세부 정보를 가져옵니다. 지정된 IAM Identity Center 권한 세트에 연결된 IAM 관리형 정책을 가져옵니다. IAM Identity	

변경 사항	설명	날짜
	Center 인스턴스에 대해 설정된 권한 가져오기 및 IAM Identity Center 리소스에 대한 태그를 가져옵니다.	
AWSConfigServiceRolePolicy – cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies 추가	이제이 정책은 전체 또는 지정된 AWS CloudTrail 이벤트 데이터 스토어(EDS)에 대한 정보를 가져오고, 전체 또는 지정된 AWS CloudFormation 리소스에 대한 정보를 가져오고, DynamoDB Accelerator(DAX) 파라미터 그룹 또는 서브넷 그룹의 목록을 가져오고, 액세스 중인 현재 리전의 계정에 대한 AWS Database Migration Service (AWS DMS) 복제 작업에 대한 정보를 가져오고, 지정된 유형의에 있는 모든 정책 목록을 가져올 수 AWS Organizations 있는 권한을 부여합니다.	2022년 4월 7일

변경 사항	설명	날짜
AWS_ConfigRole – cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies 추가	이제이 정책은 전체 또는 지정된 AWS CloudTrail 이벤트 데이터 스토어(EDS)에 대한 정보를 가져오고, 전체 또는 지정된 AWS CloudFormation 리소스에 대한 정보를 가져오고, DynamoDB Accelerator(DAX) 파라미터 그룹 또는 서브넷 그룹의 목록을 가져오고, 액세스 중인 현재 리전의 계정에 대한 AWS Database Migration Service (AWS DMS) 복제 작업에 대한 정보를 가져오고, 지정된 유형의에 있는 모든 정책 목록을 가져올 수 AWS Organizations 있는 권한을 부여합니다.	2022년 4월 7일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	이제이 정책은 AWS Backup, AWS Batch DynamoDB Accelerator, AWS Database Migration Service Amazon DynamoDB, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx, Amazon GuardDuty, AWS Key Management Service AWS OpsWorks, Amazon Relational Database Service, AWS WAF V2 및 Amazon WorkSpaces에 대한 추가 권한을 지원합니다.	2022년 3월 14일

변경 사항	설명	날짜
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces 추가		

변경 사항	설명	날짜
AWS_ConfigRole – backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct	이제이 정책은 AWS Backup, AWS Batch DynamoDB Accelerator, AWS Database Migration Service Amazon DynamoDB, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx, Amazon GuardDuty , AWS Key Management Service AWS OpsWorks, Amazon Relational Database Service, AWS WAF V2 및 Amazon WorkSpaces에 대한 추가 권한을 지원합니다.	2022년 3월 14일

변경 사항	설명	날짜
ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces 추가		

변경 사항	설명	날짜
AWSConfigServiceRolePolicy – elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies 추가	이 정책은 이제 Elastic Beanstalk 환경에 대한 세부 정보 및 지정된 Elastic Beanstalk 구성 세트의 설정에 대한 설명을 가져오고, OpenSearch 또는 Elasticsearch 버전의 맵을 가져오고, 데이터베이스에 사용할 수 있는 Amazon RDS 옵션 그룹을 설명하고, CodeDeploy 배포 구성에 대한 정보를 가져올 수 있는 권한을 부여합니다. 또한이 정책은에 연결된 지정된 대체 연락처를 검색하고 AWS 계정, AWS Organizations 정책에 대한 정보를 검색하고, Amazon ECR 리포지토리 정책을 검색하고, 아카이브된 AWS Config 규칙에 대한 정보를 검색하고, Amazon ECS 태스크 정의 패밀리 목록을 검색하고, 지정된 하위 OUs 또는 계정의 루트 또는 상위 조직 단위(OU)를 나열하고, 지정된 대상 루트, 조직 단위 또는 계정에 연결된 정책을 나열할 수 있는 권한을 부여합니다.	2022년 2월 10일

변경 사항	설명	날짜
AWS_ConfigRole – elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies 추가	이 정책은 이제 Elastic Beanstalk 환경에 대한 세부 정보 및 지정된 Elastic Beanstalk 구성 세트의 설정에 대한 설명을 가져오고, OpenSearch 또는 Elasticsearch 버전의 맵을 가져오고, 데이터베이스에 사용할 수 있는 Amazon RDS 옵션 그룹을 설명하고, CodeDeploy 배포 구성에 대한 정보를 가져올 수 있는 권한을 부여합니다. 또한이 정책은에 연결된 지정된 대체 연락처를 검색하고 AWS 계정, AWS Organizations 정책에 대한 정보를 검색하고, Amazon ECR 리포지토리 정책을 검색하고, 아카이브된 AWS Config 규칙에 대한 정보를 검색하고, Amazon ECS 태스크 정의 패밀리 목록을 검색하고, 지정된 하위 OUs 또는 계정의 루트 또는 상위 조직 단위(OU)를 나열하고, 지정된 대상 루트, 조직 단위 또는 계정에 연결된 정책을 나열할 수 있는 권한을 부여합니다.	2022년 2월 10일
AWSConfigServiceRolePolicy – logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent 추가	이 정책은 이제 Amazon CloudWatch 로그 그룹 및 스트림을 생성하고 생성된 로그 스트림에 로그를 쓸 수 있는 권한을 부여합니다.	2021년 12월 15일

변경 사항	설명	날짜
AWS_ConfigRole – logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent 추가	이 정책은 이제 Amazon CloudWatch 로그 그룹 및 스트림을 생성하고 생성된 로그 스트림에 로그를 쓸 수 있는 권한을 부여합니다.	2021년 12월 15일
AWSConfigServiceRolePolicy – es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots 추가	이 정책은 이제 Amazon OpenSearch Service(OpenSearch Service) 도메인에 대한 세부 정보를 가져오고 특정 Amazon Relational Database Service(Amazon RDS) DB 파라미터 그룹에 대한 세부 파라미터 목록을 가져올 수 있는 권한을 부여합니다. 또한 이 정책은 Amazon ElastiCache 스냅샷에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	2021년 9월 8일
AWS_ConfigRole – es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots 추가	이 정책은 이제 Amazon OpenSearch Service(OpenSearch Service) 도메인에 대한 세부 정보를 가져오고 특정 Amazon Relational Database Service(Amazon RDS) DB 파라미터 그룹에 대한 세부 파라미터 목록을 가져올 수 있는 권한을 부여합니다. 또한 이 정책은 Amazon ElastiCache 스냅샷에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다.	2021년 9월 8일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy - logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine, 리소스 AWS 유형에 대한 추가 권한 추가	이 정책은 이제 로그 그룹의 태그를 나열하고, 상태 시스템의 태그를 나열하고, 모든 상태 시스템을 나열할 수 있는 권한을 부여합니다. 이 정책은 이제 상태 시스템에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다. 이 정책은 이제 Amazon EC2 Systems Manager(SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon Relational Database Service(RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notificat ion Service AWS Database Migration Service, AWS Global Accelerator및에 대한 추가 권한도 지원합니다 AWS Storage Gateway.	2021년 7월 28일

변경 사항	설명	날짜
AWS_ConfigRole - AWS 리소스 유형에 대한 l ogs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine및 추가 권한 추가	이 정책은 이제 로그 그룹의 태그를 나열하고, 상태 시스템의 태그를 나열하고, 모든 상태 시스템을 나열할 수 있는 권한을 부여합니다. 이 정책은 이제 상태 시스템에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다. 이 정책은 이제 Amazon EC2 Systems Manager(SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon Relational Database Service(RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notification Service AWS Database Migration Service, AWS Global Accelerator및에 대한 추가 권한도 지원합니다 AWS Storage Gateway.	2021년 7월 28일

변경 사항	설명	날짜
AWSConfigServiceRolePolicy - AWS 리소스 유형에 대한 ssm:DescribeDocumentPermission 및 추가 권한 추가	이 정책은 이제 AWS Systems Manager 문서의 권한 및 IAM Access Analyzer에 대한 정보를 볼 수 있는 권한을 부여합니다. 이제이 정책은 Amazon Kinesis, Amazon ElastiCache, Amazon EMR AWS Network Firewall, Amazon Route 53 및 Amazon Relational Database Service(RDS)에 대한 추가 AWS 리소스 유형을 지원합니다. 이러한 권한 변경을 통해는 이러한 리소스 유형을 지원하는 데 필요한 읽기 전용 APIs AWS Config 호출할 수 있습니다. 이 정책은 이제 lambda-inside-vpc 관리형 규칙에 대한 Lambda AWS Config @Edge 함수 필터링도 지원합니다.	2021년 6월 8일

변경 사항	설명	날짜
AWS_ConfigRole - AWS 리소스 유형에 대한 ssm:DescribeDocumentPermission 및 추가 권한 추가	이 정책은 이제 AWS Systems Manager 문서의 권한 및 IAM Access Analyzer에 대한 정보를 볼 수 있는 권한을 부여합니다. 이제이 정책은 Amazon Kinesis, Amazon ElastiCache, Amazon EMR AWS Network Firewall, Amazon Route 53 및 Amazon Relational Database Service(RDS)에 대한 추가 AWS 리소스 유형을 지원합니다. 이러한 권한 변경을 통해는 이러한 리소스 유형을 지원하는 데 필요한 읽기 전용 APIs AWS Config 호출할 수 있습니다. 이 정책은 이제 lambda-inside-vpc 관리형 규칙에 대한 Lambda AWS Config @Edge 함수 필터링도 지원합니다.	2021년 6월 8일
AWSConfigServiceRolePolicy - API Gateway에 읽기 전용 GET 직접 호출을 수행할 수 있는 apigateway:GET 권한 및 Amazon S3 읽기 전용 API를 간접 호출할 수 있는 s3:GetAccessPointPolicy 권한 및 s3:GetAccessPointPolicyStatus 권한을 추가	이제이 정책은가 API Gateway AWS Config 에 대한 AWS Config 규칙을 지원하기 위해 API Gateway에 대한 읽기 전용 GET 호출을 수행할 수 있는 권한을 부여합니다. 또한 이 정책은가 새 `AWS::S3::AccessPoint` 리소스 유형을 지원하는 AWS Config 데 필요한 Amazon Simple Storage Service(Amazon S3) 읽기 전용 APIs를 호출할 수 있는 권한을 추가합니다.	2021년 5월 10일

변경 사항	설명	날짜
AWS_ConfigRole - API Gateway에 읽기 전용 GET 호출을 수행할 수 있는 apigateway:GET 권한 및 Amazon S3 읽기 전용 API를 간접 호출할 수 있는 s3:GetAccessPointPolicy 권한 및 s3:GetAccessPointPolicyStatus 권한을 추가	이제이 정책은가 API Gateway AWS Config 용 AWS Config 를 지원하기 위해 API Gateway 에 대한 읽기 전용 GET 호출을 수행할 수 있는 권한을 부여합니다. 또한이 정책은가 새 `AWS::S3::AccessPoint` 리소스 유형을 지원하는 AWS Config 데 필요한 Amazon Simple Storage Service(Amazon S3) 읽기 전용 APIs를 호출할 수 있는 권한을 추가합니다.	2021년 5월 10일
AWSConfigServiceRolePolicy - AWS 리소스 유형에 대한 ssm:ListDocuments 권한 및 추가 권한 추가	이 정책은 이제 AWS Systems Manager 에서 지정된 문서에 대한 정보를 볼 수 있는 권한을 부여합니다. 이 정책은 이제 Amazon Elastic File System AWS Backup, Amazon ElastiCache, Amazon Simple Storage Service(Amazon S3), Amazon Elastic Compute Cloud(Amazon EC2), Amazon Kinesis, Amazon SageMaker AI AWS Database Migration Service및 Amazon Route 53에 대한 추가 AWS 리소스 유형도 지원합니다. 이러한 권한 변경을 통해는 이러한 리소스 유형을 지원하는 데 필요한 읽기 전용 APIs AWS Config 호출할 수 있습니다.	2021년 4월 1일

변경 사항	설명	날짜
AWS_ConfigRole - AWS 리소스 유형에 대한 ssm:ListDocuments 권한 및 추가 권한 추가	이 정책은 이제 AWS Systems Manager 에서 지정된 문서에 대한 정보를 볼 수 있는 권한을 부여합니다. 이 정책은 이제 Amazon Elastic File System AWS Backup, Amazon ElastiCache, Amazon Simple Storage Service(Amazon S3), Amazon Elastic Compute Cloud(Amazon EC2), Amazon Kinesis, Amazon SageMaker AI AWS Database Migration Service및 Amazon Route 53에 대한 추가 AWS 리소스 유형도 지원합니다. 이러한 권한 변경을 통해는 이러한 리소스 유형을 지원하는 데 필요한 읽기 전용 APIs AWS Config 호출할 수 있습니다.	2021년 4월 1일
`AWSConfigRole` 은 더 이상 사용되지 않습니다.	`AWSConfigRole` 은 더 이상 사용되지 않습니다. 대체 정책은 `AWS_ConfigRole` 입니다.	2021년 4월 1일
AWS Config 에서 변경 내용 추적 시작	AWS Config 가 AWS 관리형 정책에 대한 변경 내용 추적을 시작했습니다.	2021년 4월 1일

에 할당된 IAM 역할에 대한 권한 AWS Config

IAM 역할을 사용하면 권한 세트를 정의할 수 있습니다.는 S3 버킷에 쓰고, SNS 주제에 게시하고, AWS 리소스에 대한 구성 세부 정보를 가져오기 위해 `Describe` 또는 `List` API 요청을 하기 위해 할당한 역할을 수 AWS Config 임합니다. IAM 역할에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 섹션을 참조하세요.

AWS Config 콘솔을 사용하여 IAM 역할을 생성하거나 업데이트하면가 필요한 권한을 AWS Config 자동으로 연결합니다. 자세한 내용은 콘솔 AWS Config 로 설정 단원을 참조하십시오.

> **정책 및 규정 준수 결과**
>
> 에서 관리되는 IAM 정책 및 기타 정책은에 리소스에 대한 구성 변경을 기록할 권한이 있는지 여부에 AWS Config 영향을 미칠 수 있습니다. AWS Organizations 또한 규칙은 리소스의 구성을 직접 평가하며, 규칙은 평가를 실행할 때 이러한 정책을 고려하지 않습니다. 적용 중인 정책이 사용 의도와 일치하는지 확인합니다 AWS Config.

목차

- IAM 역할 정책 생성
  - 역할에 IAM 신뢰 정책 추가
  - S3 버킷에 대한 IAM 역할 정책
  - KMS 키에 대한 IAM 역할 정책
  - Amazon SNS 주제에 대한 IAM 역할 정책
  - 구성 세부 정보를 가져오기 위한 IAM 역할 정책
  - S3 버킷 기록에 대한 권한 관리

IAM 역할 정책 생성

AWS Config 콘솔을 사용하여 IAM 역할을 생성하면가 필요한 권한을 역할에 AWS Config 자동으로 연결합니다.

를 사용하여 AWS CLI 를 설정 AWS Config 하거나 기존 IAM 역할을 업데이트하는 경우가 S3 버킷에 AWS Config 액세스하고 SNS 주제에 게시하며 리소스에 대한 구성 세부 정보를 가져올 수 있도록 정책을 수동으로 업데이트해야 합니다.

역할에 IAM 신뢰 정책 추가

가 역할을 AWS Config 수임하고 이를 사용하여 리소스를 추적할 수 있도록 하는 IAM 신뢰 정책을 생성할 수 있습니다. 신뢰 정책에 대한 자세한 내용은 IAM 사용 설명서의 역할 용어 및 개념을 참조하세요.

다음은 AWS Config 역할에 대한 신뢰 정책의 예입니다.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

위의 IAM 역할 신뢰 관계의 `AWS:SourceAccount` 조건을 사용하여 특정 계정을 대신하여 작업을 수행할 때 Config 서비스 보안 주체가 AWS IAM 역할과만 상호 작용하도록 제한할 수 있습니다.

AWS Config 는 소유 계정을 대신하여 작업을 수행할 때 Config 서비스 보안 주체가 IAM 역할만 수임하도록 제한하는 `AWS:SourceArn` 조건도 지원합니다. AWS Config 서비스 보안 주체를 사용할 때 `AWS:SourceArn` 속성은 항상 로 설정됩니다. `arn:aws:config:sourceRegion:sourceAccountID:*` 여기서 `sourceRegion`는 고객 관리형 구성 레코더의 리전이고 `sourceAccountID`는 고객 관리형 구성 레코더가 포함된 계정의 ID입니다.

예를 들어 Config 서비스 보안 주체가 계정의 `us-east-1` 리전에 있는 고객 관리형 구성 레코더를 대신하여 IAM 역할만 수임하도록 제한하는 조건을 추가합니다`123456789012``"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

S3 버킷에 대한 IAM 역할 정책

다음 예제 정책은 S3 버킷에 액세스할 수 있는 AWS Config 권한을 부여합니다.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
```

```
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

KMS 키에 대한 IAM 역할 정책

다음 예제 정책은 S3 버킷 전송을 위해 새 객체에 KMS 기반 암호화를 사용할 수 있는 AWS Config 권한을 부여합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN"
        }
    ]
}
```

Amazon SNS 주제에 대한 IAM 역할 정책

다음 예제 정책은 SNS 주제에 액세스할 수 있는 AWS Config 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"mySNStopicARN"
     }
    ]
}
```

SNS 주제가 암호화된 경우 추가 설정 지침은 Amazon Simple Notification Service 개발자 안내서의 AWS KMS 권한 구성을 참조하세요.

구성 세부 정보를 가져오기 위한 IAM 역할 정책

AWS Config 서비스 연결 역할인를 사용하는 것이 좋습니다`AWSServiceRoleForConfig`. 서비스 연결 역할은 사전 정의되며가 다른를 호출하는 데 AWS Config 필요한 모든 권한을 포함합니다 AWS 서비스. AWS Config 서비스 연결 구성 레코더에는 서비스 연결 역할이 필요합니다. 자세한 내용은 AWS Config에 대한 서비스 연결 역할 사용을 참조하십시오.

콘솔을 사용하여 역할을 생성하거나 업데이트하면 AWS Config 가 AWSServiceRoleForConfig를 연결합니다.

를 사용하는 경우 `attach-role-policy` 명령을 AWS CLI사용하고 AWSServiceRoleForConfig의 Amazon 리소스 이름(ARN)을 지정합니다.

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn
 arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForConfig
```

S3 버킷 기록에 대한 권한 관리

AWS Config 는 S3 버킷이 생성, 업데이트 또는 삭제될 때 알림을 기록하고 전송합니다.

AWS Config 서비스 연결 역할인를 사용하는 것이 좋습니다`AWSServiceRoleForConfig`. 서비스 연결 역할은 사전 정의되며가 다른를 호출하는 데 AWS Config 필요한 모든 권한을 포함합니다 AWS 서비스. AWS Config 서비스 연결 구성 레코더에는 서비스 연결 역할이 필요합니다. 자세한 내용은 AWS Config에 대한 서비스 연결 역할 사용을 참조하십시오.

고객 관리형 구성 레코더의 IAM 역할 업데이트

고객 관리형 구성 레코더에서 사용하는 IAM 역할을 업데이트할 수 있습니다. IAM 역할을 업데이트하기 전에 이전 역할을 대체하는 새 역할을 생성해야 합니다. 구성을 기록하고 전송 채널로 전달할 수 있는 권한을 AWS Config 에 부여하는 정책을 새 역할에 연결해야 합니다.

IAM 역할을 생성하고 IAM 역할에 필요한 정책을 연결하는 방법에 대한 자세한 내용은 3단계: IAM 역할 생성 섹션을 참조하세요.

> **Note**
>
> 기존 IAM 역할의 ARN을 찾으려면 IAM 콘솔(https://console.aws.amazon.com/iam/)로 이동합니다. 탐색 창에서 역할을 선택합니다. 그런 다음 원하는 역할 이름을 선택하고 요약 페이지 상단에서 해당 ARN을 찾습니다.

IAM 역할 업데이트

AWS Management Console 또는를 사용하여 IAM 역할을 업데이트할 수 있습니다 AWS CLI.

To update the IAM role (Console)

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/config/home AWS Config 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택합니다.
3. 고객 관리형 레코더 탭의 설정 페이지에서 편집을 선택합니다.
4. 데이터 거버넌스 섹션에서 AWS Config다음에 대한 IAM 역할을 선택합니다.
   - 기존 AWS Config 서비스 연결 역할 사용 - 필요한 권한이 있는 역할을 AWS Config 생성합니다.
   - 계정에서 역할 선택 - 계정에서 기존 역할에 대한 IAM 역할을 선택합니다.
5. 저장을 선택합니다.

To update the IAM role (AWS CLI)

다음 `put-configuration-recorder` 명령을 사용하여 새 역할의 Amazon 리소스 이름(ARN)을 지정합니다.

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

AWS Config 전송 채널에 대한 Amazon S3 버킷에 대한 권한

> **Important**
>
> 이 페이지에서는 AWS Config 전송 채널에 대한 Amazon S3 버킷을 설정합니다. 이 페이지는 AWS Config 구성 레코더가 기록할 수 있는 `AWS::S3::Bucket` 리소스 유형에 대한 것이 아닙니다.

Amazon S3 버킷 및 객체는 기본적으로 프라이빗입니다. 버킷 AWS 계정 (리소스 소유자)을 생성한 에만 액세스 권한이 있습니다. 리소스 소유자는 액세스 정책을 생성하여 다른 리소스 및 사용자에게 액세스 권한을 부여할 수 있습니다.

가 AWS Config 자동으로 S3 버킷을 생성하면 필요한 권한이 추가됩니다. 그러나 기존 S3 버킷을 지정하는 경우 이러한 권한을 수동으로 추가해야 합니다.

주제

- IAM 역할을 사용할 때 Amazon S3 버킷에 필요한 권한
- 서비스 연결 역할을 사용할 때 Amazon S3 버킷에 필요한 권한
- Amazon S3 버킷에 대한 AWS Config 액세스 권한 부여
- 교차 계정을 전송할 때 Amazon S3 버킷에 필요한 권한

IAM 역할을 사용할 때 Amazon S3 버킷에 필요한 권한

AWS Config 는 구성 레코더에 할당한 IAM 역할을 사용하여 계정의 S3 버킷에 구성 기록 및 스냅샷을 전달합니다. 교차 계정 전송의 경우 AWS Config 먼저 할당된 IAM 역할을 사용하려고 시도합니다. 버킷 정책이 IAM 역할에 대한 `WRITE` 액세스 권한을 부여하지 않으면는 `config.amazonaws.com` 서비스 보안 주체를 AWS Config 사용합니다. 버킷 정책은 전송을 완료하기 `config.amazonaws.com` 위해에 `WRITE` 액세스 권한을 부여해야 합니다. 전송에 성공하면는 교차 계정 S3 버킷에 전달하는 모든 객체의 소유권을 AWS Config 유지합니다.

AWS Config 는 구성 레코더에 할당한 IAM 역할로 Amazon S3 HeadBucket API를 호출하여 S3 버킷의 존재 여부와 위치를 확인합니다. 에서 확인하는 AWS Config 데 필요한 권한이 없는 경우 AWS

CloudTrail 로그에 `AccessDenied` 오류가 표시됩니다. 그러나는에 S3 버킷이 존재하는지 여부와 그 위치를 확인하는 데 필요한 권한이 AWS Config 없더라도 구성 기록과 스냅샷을 AWS Config 전달할 수 있습니다.

> **최소 권한**
>
> Amazon S3 `HeadBucket` API에는 `s3:ListBucket` 작업이 필요합니다.

서비스 연결 역할을 사용할 때 Amazon S3 버킷에 필요한 권한

AWS Config 서비스 연결 역할에는 Amazon S3 버킷에 객체를 넣을 수 있는 권한이 없습니다. 서비스 연결 역할을 AWS Config 사용하여를 설정하면 AWS Config 는 `config.amazonaws.com` 서비스 보안 주체를 사용하여 구성 기록 및 스냅샷을 제공합니다. 계정 또는 교차 계정 대상의 S3 버킷 정책에는 AWS Config 서비스 보안 주체가 객체를 작성할 수 있는 권한이 포함되어야 합니다.

Amazon S3 버킷에 대한 AWS Config 액세스 권한 부여

다음 단계를 완료 AWS Config 하면가 Amazon S3 버킷에 구성 기록 및 스냅샷을 전달할 수 있습니다.

1. S3 버킷이 있는 계정을 AWS Management Console 사용하여에 로그인합니다.
2. https://console.aws.amazon.com/s3/에서 S3 콘솔을 엽니다.
3. 구성 항목을 전달하는 데 사용할 버킷 AWS Config 을 선택한 다음 속성을 선택합니다.
4. 권한을 선택합니다.
5. [Edit Bucket Policy]를 선택합니다.
6. 다음 정책을 버킷 정책 편집기 창으로 복사합니다.

> **보안 모범 사례**
>
> `AWS:SourceAccount` 조건으로 버킷 정책의 액세스를 제한하는 것이 좋습니다. 이렇게 하면 AWS Config 가 예상 사용자만을 대신하여 액세스 권한을 부여받습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
```

```
}
```

7. 버킷 정책에서 다음 값을 바꿉니다.
   - *amzn-s3-demo-bucket* - AWS Config 가 구성 기록 및 스냅샷을 제공하는 Amazon S3 버킷의 이름입니다.
   - *[## ##] prefix* - Amazon S3 버킷 안에 폴더 같은 조직을 만들기 위해 객체 키에 선택적으로 추가할 수 있습니다.
   - *sourceAccountID* - AWS Config 가 구성 기록 및 스냅샷을 전송하는 계정의 ID입니다.
8. 저장을 선택한 후 닫기를 선택합니다.

`AWS:SourceAccount` 조건은 AWS Config 작업을 지정된 로 제한합니다 AWS 계정. 단일 S3 버킷에 전달하는 조직 내 다중 계정 구성의 경우 서비스 연결 역할 대신 AWS Organizations 조건 키가 있는 IAM 역할을 사용합니다. 예를 들어 `AWS:PrincipalOrgID`입니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직에 대한 액세스 권한 관리를 참조하세요.

`AWS:SourceArn` 조건은 지정된 전송 채널로 AWS Config 작업을 제한합니다. `AWS:SourceArn` 형식은 입니다`arn:aws:config:`*sourceRegion*`:`*123456789012*.

예를 들어 계정 123456789012의 미국 동부(버지니아 북부) 리전에 있는 전송 채널에 대한 S3 버킷 액세스를 제한하려면 다음 조건을 추가합니다.

```
"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:"}
```

교차 계정을 전송할 때 Amazon S3 버킷에 필요한 권한

AWS Config 가 구성 기록과 스냅샷을 다른 계정의 Amazon S3 버킷에 전송하도록 구성된 경우(교차 계정 설정), 전송 채널에 지정된 구성 레코더와 S3 버킷이 서로 다른 경우 AWS 계정다음 권한이 필요합니다.

- 구성 레코더에 할당하는 IAM 역할에는 `s3:ListBucket` 작업을 수행할 수 있는 명시적 권한이 필요합니다. 이는가이 IAM 역할로 Amazon S3 HeadBucket API를 AWS Config 호출하여 버킷 위치를 결정하기 때문입니다.
- S3 버킷 정책에는 AWS Config 서비스 보안 주체와 구성 레코더에 할당된 IAM 역할 모두에 대한 권한이 포함되어야 합니다.

다음은 버킷 정책 구성의 예입니다.

```
{
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com",
        "AWS": "IAM Role-Arn assigned to the configuration recorder"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
}
```

AWS Config 전송 채널의 KMS 키에 대한 권한

S3 버킷 전송을 위해에서 제공하는 객체에 KMS 기반 암호화를 사용할 수 있도록 S3 버킷 AWS Config 의 AWS KMS 키에 대한 정책을 생성하려면이 주제의 정보를 사용합니다.

목차

- IAM 역할을 사용할 때 KMS 키에 필요한 권한(S3 버킷 전송)
- 서비스 연결 역할을 사용할 때 AWS KMS 키에 필요한 권한(S3 버킷 전송)
- AWS KMS 키에 대한 AWS Config 액세스 권한 부여

IAM 역할을 사용할 때 KMS 키에 필요한 권한(S3 버킷 전송)

IAM 역할을 AWS Config 사용하여를 설정하는 경우 KMS 키에 다음 권한 정책을 연결할 수 있습니다.

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

> **Note**
>
> IAM 역할, Amazon S3 버킷 정책 또는 AWS KMS 키가에 대한 적절한 액세스를 제공하지 않으면 Amazon S3 버킷으로 구성 정보를 보내 AWS Config AWS Config려는 시도가 실패합니다. 이 경우는 이번에는 AWS Config 서비스 보안 주체로 정보를 다시 AWS Config 전송합니다. 이 경우 아래에 언급된 권한 정책을 AWS KMS 키에 연결하여 Amazon S3 버킷에 정보를 전송할 때 키를 사용할 수 있는 AWS Config 액세스 권한을 부여해야 합니다.

서비스 연결 역할을 사용할 때 AWS KMS 키에 필요한 권한(S3 버킷 전송)

AWS Config 서비스 연결 역할에는 AWS KMS 키에 액세스할 수 있는 권한이 없습니다. 따라서 서비스 연결 역할을 AWS Config 사용하여를 설정하면 AWS Config 가 대신 서비스 보안 주체로 AWS Config 정보를 전송합니다. Amazon S3 버킷에 정보를 전송할 때 AWS KMS 키를 사용할 수 있는 액세스 권한을 부여하려면 아래에 언급된 AWS Config 액세스 정책을 AWS KMS 키에 연결해야 합니다.

AWS KMS 키에 대한 AWS Config 액세스 권한 부여

이 정책은가 Amazon S3 버킷 AWS Config 에 정보를 전송할 때 AWS KMS 키를 사용하도록 허용합니다.

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

키 정책에서 다음 값을 바꿉니다.

- *myKMSKeyARN* - 구성 항목을 전달할 Amazon S3 버킷의 데이터를 암호화하는 데 사용되는 AWS KMS 키의 ARN AWS Config 입니다.
- *sourceAccountID* - AWS Config 가 구성 항목을 전송할 계정의 ID입니다.

위의 AWS KMS 키 정책의 `AWS:SourceAccount` 조건을 사용하여 특정 계정을 대신하여 작업을 수행할 때 Config 서비스 보안 주체가 AWS KMS 키와만 상호 작용하도록 제한할 수 있습니다.

AWS Config 는 특정 AWS Config 전송 채널을 대신하여 작업을 수행할 때 Config 서비스 보안 주체가 Amazon S3 버킷과만 상호 작용하도록 제한하는 `AWS:SourceArn` 조건도 지원합니다. AWS Config 서비스 보안 주체를 사용하는 경우 `AWS:SourceArn` 속성은 항상 로 설정됩니다. `arn:aws:config:sourceRegion:sourceAccountID:*` 여기서 `sourceRegion`는 전송 채널의 리전이고 `sourceAccountID`는 전송 채널이 포함된 계정의 ID입니다. AWS Config 전송 채널에 대한 자세한 내용은 전송 채널 관리를 참조하세요. 예를 들어, 다음 조건을 추가하여 Config 서비스 보안 주체가 `123456789012` 계정의 `us-east-1` 리전 전송 채널을 대신해서만 Amazon S3 버킷과 상호 작용하도록 제한할 수 있습니다. `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Amazon SNS 주제에 대한 권한

이 주제에서는 다른 계정이 소유한 Amazon SNS 주제를 전달 AWS Config 하도록를 구성하는 방법을 설명합니다. Amazon SNS 주제에 알림을 보내는 데 필요한 권한이 있어야 AWS Config 합니다.

AWS Config 콘솔에서 새 Amazon SNS 주제를 생성하면는 필요한 권한을 AWS Config 부여합니다. 기존 Amazon SNS 주제를 선택하는 경우 Amazon SNS 주제에 필요한 권한이 포함되어 있고 보안 모범 사례를 따르는지 확인합니다.

> 리전 간 Amazon SNS 주제는 지원되지 않습니다.
>
> AWS Config 는 현재 동일한 및 계정 AWS 리전 간 액세스만 지원합니다.

목차

- IAM 역할을 사용할 때 Amazon SNS 주제에 필요한 권한
- 서비스 연결 역할을 사용할 때 Amazon SNS 주제에 필요한 권한
- Amazon SNS 주제에 대한 AWS Config 액세스 권한 부여
- Amazon SNS 주제 문제 해결

IAM 역할을 사용할 때 Amazon SNS 주제에 필요한 권한

다른 계정에서 소유한 Amazon SNS 주제에 권한 정책을 연결할 수 있습니다. 다른 계정의 Amazon SNS 주제를 사용하고자 하는 경우, 기존 Amazon SNS 주제에 다음 정책을 연결해야 합니다.

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
```

```
}
```

`Resource` 키의 경우, *`account-id`*는 주제 소유자의 AWS 계정 번호입니다. *`account-id1`*, *`account-id2`* 및 *`account-id3`*에 Amazon SNS 주제에 데이터를 전송할 AWS 계정 을 사용합니다. *`region`* 및 *`myTopic`*을 적절한 값으로 바꿀 수 있습니다.

가 Amazon SNS 주제에 알림을 AWS Config 보낼 때 먼저 IAM 역할을 사용하려고 시도하지만 역할 또는에 주제에 게시할 권한이 없는 경우이 시도 AWS 계정 는 실패합니다. 이 경우는 이번에는 AWS Config 서비스 보안 주체 이름(SPN)으로 알림을 다시 AWS Config 보냅니다. 게시가 성공하려면 먼저 주제의 액세스 정책이 `sns:Publish`에게 `config.amazonaws.com` 보안 주체 이름에 액세스할 수 있는 권한을 부여해야 합니다. IAM 역할이 주제에 게시할 권한이 없는 경우 다음 섹션에서 설명하는 액세스 정책을 Amazon SNS 주제에 연결하여 AWS Config 에게 Amazon SNS 주제에 액세스할 수 있는 권한을 부여해야 합니다.

서비스 연결 역할을 사용할 때 Amazon SNS 주제에 필요한 권한

AWS Config 서비스 연결 역할에는 Amazon SNS 주제에 액세스할 수 있는 권한이 없습니다. 따라서 서비스 연결 역할(SLR)을 AWS Config 사용하여를 설정하면 AWS Config 가 대신 서비스 보안 주체로 AWS Config 정보를 전송합니다. Amazon SNS 주제에 정보를 전송할 수 있는 액세스 권한을 부여하려면 아래에 언급된 AWS Config 액세스 정책을 Amazon SNS 주제에 연결해야 합니다.

동일 계정 설정의 경우, Amazon SNS 주제와 SLR이 동일한 계정에 있고 Amazon SNS 정책이 SLR에게 '`sns:Publish`' 권한을 부여하면 AWS Config SPN을 사용할 필요가 없습니다. 아래의 권한 정책 및 보안 모범 사례 권장 사항은 교차 계정 설정을 위한 것입니다.

Amazon SNS 주제에 대한 AWS Config 액세스 권한 부여

이 정책은가 Amazon SNS 주제에 알림을 AWS Config 보내도록 허용합니다. 다른 계정에서 Amazon SNS 주제에 대한 AWS Config 액세스 권한을 부여하려면 다음 권한 정책을 연결해야 합니다.

> **Note**
>
> 보안 모범 사례로 조건에 나열된 계정에 대한 액세스를 제한하여 AWS Config 가 예상 사용자를 대신하여 리소스에 액세스하는지 확인하는 것이 좋습니다`AWS:SourceAccount`.

```
{
"Id": "Policy_ID",
```

```
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

`Resource` 키의 경우, *`account-id`*는 주제 소유자의 AWS 계정 번호입니다. *`account-id1`*, *`account-id2`* 및 *`account-id3`*에 Amazon SNS 주제에 데이터를 전송할 AWS 계정 을 사용합니다. *`region`* 및 *`myTopic`*을 적절한 값으로 바꿀 수 있습니다.

이전 Amazon SNS 주제 정책의 `AWS:SourceAccount` 조건을 사용하여 특정 계정을 대신하여 작업을 수행할 때 AWS Config 서비스 보안 주체 이름(SPN)이 Amazon SNS 주제와만 상호 작용하도록 제한할 수 있습니다.

AWS Config 는 특정 AWS Config 전송 채널을 대신하여 작업을 수행할 때 서비스 보안 주체 이름(SPN)이 S3 버킷과만 상호 작용하도록 제한 AWS Config 하는 `AWS:SourceArn` 조건도 지원합니다. AWS Config 서비스 보안 주체 이름(SPN)을 사용하는 경우 `AWS:SourceArn` 속성은 항상 로 설정됩니다. `arn:aws:config:sourceRegion:sourceAccountID:*` 여기서 `sourceRegion`는 전송 채널의 리전이고 `sourceAccountID`는 전송 채널이 포함된 계정의 ID입니다. AWS Config 전송 채널에 대한 자세한 내용은 전송 채널 관리를 참조하세요. 예를 들어, AWS Config 서비스 보안 주체 이름(SPN)이 계정의 `us-east-1` 리전에 있는 전송 채널을 대신하여만 S3 버킷과 상호 작용하도록 제한하려면 `123456789012`다음 조건을 추가합니다`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Amazon SNS 주제 문제 해결

AWS Config 에는 Amazon SNS 주제에 알림을 보낼 수 있는 권한이 있어야 합니다. Amazon SNS 주제가 알림을 수신할 수 없는 경우 AWS Config 수임 중인 IAM 역할에 필요한 `sns:Publish` 권한이 있는지 확인합니다.

AWS Config 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단 AWS Config 하고 수정할 수 있습니다.

주제

- 에서 작업을 수행할 권한이 없음 AWS Config
- iam:PassRole을 수행하도록 인증되지 않음
- 내 외부의 사람이 내 AWS Config 리소스에 액세스 AWS 계정 하도록 허용하고 싶습니다.

에서 작업을 수행할 권한이 없음 AWS Config

작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `config:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 config:GetWidget on resource: my-example-widget
```

이 경우 Mateo의 정책은 `config:`*`GetWidget`* 작업을 사용하여 *`my-example-widget`* 리소스에 액세스하도록 허용하도록 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행하도록 인증되지 않음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 AWS Config에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 AWS Config에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 `iam:PassRole` 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 AWS Config 리소스에 액세스 AWS 계정 하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 에서 이러한 기능을 AWS Config 지원하는지 여부를 알아보려면 섹션을 참조하세요AWS Config 에서 IAM을 사용하는 방법.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

에 서비스 연결 역할 사용 AWS Config

AWS Config 는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결된 고유한 유형의 IAM 역할입니다 AWS Config. 서비스 연결 역할은에서 사전 정의 AWS Config 하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할을 더 AWS Config 쉽게 설정할 수 있습니다.는 서비스 연결 역할의 권한을 AWS Config 정의하며, 달리 정의되지 않은 한 만 해당 역할을 수임 AWS Config 할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔티티에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조해 서비스 연결 역할(Service-Linked Role) 열이 예(Yes)인 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 링크가 있는 예를 선택합니다.

에 대한 서비스 연결 역할 권한 AWS Config

AWS Config 는 AwsServiceRoleForConfig라는 서비스 연결 역할을 사용합니다.는이 서비스 연결 역할을 AWS Config 사용하여 사용자를 대신하여 다른 AWS 서비스를 호출합니다.

AwsServiceRoleForConfig 서비스 연결 역할은 역할을 수임하기 위해 `config.amazonaws.com` 서비스를 신뢰합니다.

`AwsServiceRoleForConfig` 역할에 대한 권한 정책에는 AWS Config 리소스에 대한 읽기 전용 및 쓰기 전용 권한과가 AWS Config 지원하는 다른 서비스의 리소스에 대한 읽기 전용 권한이 포함됩니다. AwsServiceRoleForConfig에 대한 관리형 정책을 보려면에 대한 AWS 관리형 정책을 참조하세요 AWS Config.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 섹션을 참조하세요.

에서 서비스 연결 역할을 사용하려면 Amazon S3 버킷 및 Amazon SNS 주제에 대한 권한을 구성 AWS Config해야 합니다. 자세한 내용은 서비스 연결 역할을 사용할 때 Amazon S3 버킷에 필요한 권한, 서비스 연결 역할을 사용할 때 AWS KMS 키에 필요한 권한(S3 버킷 전송), 서비스 연결 역할을 사용할 때 Amazon SNS 주제에 필요한 권한 섹션을 참조하세요.

에 대한 서비스 연결 역할 생성 AWS Config

IAM CLI 또는 IAM API에서 `config.amazonaws.com` 서비스 이름의 서비스 연결 역할을 생성합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 생성 섹션을 참조하세요. 이 서비스 연결 역할을 삭제하면 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

에 대한 서비스 연결 역할 편집 AWS Config

AWS Config 에서는 AwsServiceRoleForConfig 서비스 연결 역할을 편집할 수 없습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다.

하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

에 대한 서비스 연결 역할 삭제 AWS Config

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려고 할 때 AWS Config 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AwsServiceRoleForConfig에서 사용하는 AWS Config 리소스를 삭제하려면

따라서 서비스 연결 역할을 사용하여 `ConfigurationRecorders` 이 없는지 확인합니다. AWS Config 콘솔을 사용하여 구성 레코더를 중지할 수 있습니다. 기록을 중지하려면 Recording is on 아래에서 Turn off를 선택합니다.

AWS Config API를 `ConfigurationRecorder` 사용하여를 삭제할 수 있습니다. 삭제하려면 `delete-configuration-recorder` 명령을 사용합니다.

```
$ aws configservice delete-configuration-recorder --configuration-recorder-name default
```

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 AwsServiceRoleForConfig 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

의 인시던트 대응 AWS Config

AWS에서는 보안을 가장 중요하게 생각합니다. AWS 클라우드 공동 책임 모델의 일환으로는 보안에 가장 민감한 조직의 요구 사항을 충족하는 데이터 센터, 네트워크 및 소프트웨어 아키텍처를 AWS 관리합니다. AWS 는 AWS Config 서비스 자체와 관련된 모든 인시던트 대응을 담당합니다. 또한 AWS

고객은 클라우드에서 보안을 유지할 책임이 있습니다. 즉, 액세스 권한이 있는 AWS 도구 및 기능에서 구현하도록 선택한 보안을 제어하고 공동 책임 모델의 사용자 측에서 인시던트 대응을 담당합니다.

클라우드에서 실행되는 애플리케이션의 목표를 충족하는 보안 기준을 설정하면 대응할 수 있는 편차를 감지할 수 있습니다. 보안 인시던트 대응은 복잡한 주제일 수 있으므로 인시던트 대응(IR)과 선택 사항이 기업 목표에 미치는 영향을 더 잘 이해할 수 있도록 다음 리소스를 검토하는 것이 좋습니다. AWS 보안 인시던트 대응 가이드, AWS 보안 모범 사례 백서, AWS 클라우드 채택 프레임워크(CAF)의 보안 관점 백서.

에 대한 규정 준수 검증 AWS Config

타사 감사자는 여러 AWS 규정 준수 프로그램의 AWS Config 일환으로의 보안 및 규정 준수를 평가합니다. 여기에는 SOC, PCI, FedRAMP, HIPAA 등이 포함됩니다.

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 AWS 서비스 규정 준수 프로그램 제공 범위 섹션을 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact을 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- 보안 규정 준수 및 거버넌스 - 이러한 솔루션 구현 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수 기능을 배포하는 단계를 제공합니다.
- HIPAA 적격 서비스 참조 - HIPAA 적격 서비스가 나열되어 있습니다. 모두 HIPAA 자격이 AWS 서비스 있는 것은 아닙니다.
- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 산업 및 위치에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에는 여러 프레임워크(미국 국립표준기술연구소(NIST), 결제 카드 산업 보안 표준 위원회(PCI), 국제표준화기구(ISO) 포함)의 보안 제어에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례가 요약되어 있습니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 -이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub - 내 보안 상태에 대한 포괄적인 보기를 AWS 서비스 제공합니다 AWS. Security Hub는 보안 컨트롤을 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.

- Amazon GuardDuty - 의심스러운 활동과 악의적인 활동이 있는지 환경을 모니터링하여 사용자, AWS 계정워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 따르는 데 도움을 줄 수 있습니다.
- AWS Audit Manager - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다.

의 복원력 AWS Config

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며,이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

의 인프라 보안 AWS Config

관리형 서비스인는 AWS 글로벌 네트워크 보안으로 보호 AWS Config 됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 에서 게시한 API 호출을 사용하여 네트워크를 AWS Config 통해에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 보안 암호 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 자격 증명을 생성하여 요청에 서명할 수 있습니다.

구성 및 취약성 분석

의 경우 게스트 운영 체제(OS) 및 데이터베이스 패치, 방화벽 구성, 재해 복구와 같은 기본 보안 작업을 AWS Config AWS 처리합니다.

교차 서비스 혼동된 대리자 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS교차 서비스 가장은 혼동된 대리자 문제를 초래할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 직접적으로 호출할 때 발생할 수 있습니다. 직접적으로 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS 에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

리소스 정책에서 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 컨텍스트 키를 사용하여 리소스에 다른 서비스를 AWS Config 제공하는 권한을 제한하는 것이 좋습니다. 하나의 리소스만 교차 서비스 액세스와 연결되도록 허용하려는 경우 `aws:SourceArn`를 사용하세요. 해당 계정의 모든 리소스가 교차 서비스 사용과 연결되도록 허용하려는 경우 `aws:SourceAccount`을(를) 사용합니다.

혼동된 대리자 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 `aws:SourceArn` 전역 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모르거나 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드 문자(*)를 포함한 `aws:SourceArn` 글로벌 조건 컨텍스트 키를 사용합니다. 예를 들어 `arn:aws:servicename:*:123456789012:*`입니다.

만약 `aws:SourceArn` 값에 Amazon S3 버킷 ARN과 같은 계정 ID가 포함되어 있지 않은 경우, 권한을 제한하려면 두 글로벌 조건 컨텍스트 키를 모두 사용해야 합니다.

다음 예제에서는의 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 AWS Config 방지하는 방법을 보여줍니다. Amazon S3 버킷에 AWS Config 대한 액세스 권한 부여.

에 대한 보안 모범 사례 AWS Config

AWS Config 는 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주세요.

- 태깅을 활용하여 리소스를 AWS Config더 쉽게 관리, 검색 및 필터링할 수 있습니다.
- 전송 채널이 제대로 설정되었는지 확인하고 확인되면 AWS Config 가 제대로 기록되고 있는지 확인합니다.

자세한 내용은 AWS Config 모범 사례 블로그를 참조하세요.

에서 로깅 및 모니터링 AWS Config

AWS Config 는 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다 AWS Config. 모니터링은 AWS Config 및 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다.

주제

- 를 사용하여 AWS Config API 호출 로깅 AWS CloudTrail
- 모니터링

를 사용하여 AWS Config API 호출 로깅 AWS CloudTrail

CloudTrail은에 대한 모든 API 호출을 이벤트 AWS Config 로 캡처합니다. 캡처된 호출에는 AWS Config 콘솔의 호출과 AWS Config API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 이벤트를 포함하여 CloudTrail 이벤트를 Amazon S3 버킷으로 지속적으로 전송할 수 있습니다 AWS Config. 트레일을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여에 수행된 요청, 요청이 수행된 AWS Config IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 설명은 AWS CloudTrail 사용자 가이드를 참조하십시오.

주제

- AWS Config CloudTrail의 정보
- AWS Config 로그 파일 항목 이해
- 로그 파일의 예

AWS Config CloudTrail의 정보

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. 활동이에서 발생하면 AWS Config해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 정보는 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

에 대한 이벤트를 AWS 계정포함하여에 이벤트를 지속적으로 기록하려면 추적을 AWS Config생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션의 모든 리전

에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 트레일 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에서 Amazon SNS 알림 구성
- 여러 리전으로부터 CloudTrail 로그 파일 받기 및 여러 계정으로부터 CloudTrail 로그 파일 받기

모든 AWS Config 작업은 CloudTrail에서 로깅되며 AWS Config API 참조에 문서화됩니다. 예를 들어, DeliverConfigSnapshot, DeleteDeliveryChannel 및 DescribeDeliveryChannels 작업에 대한 호출은 CloudTrail 로그 파일에 항목을 생성합니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. 자격 증명을 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청을 했는지 여부입니다.

자세한 설명은 CloudTrail userIdentity 요소를 참조하세요.

AWS Config 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

로그 파일의 예

CloudTrail 로그 항목의 예는 다음 주제를 참조하세요.

DeleteDeliveryChannel

다음 예제는 DeleteDeliveryChannel 작업에 대한 CloudTrail 로그 파일입니다.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DeliverConfigSnapshot

다음 예제는 DeliverConfigSnapshot 작업에 대한 CloudTrail 로그 파일입니다.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
```

```
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```

DescribeConfigurationRecorderStatus

다음 예제는 DescribeConfigurationRecorderStatus 작업에 대한 CloudTrail 로그 파일입니다.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
```

```
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeConfigurationRecorders

다음 예제는 DescribeConfigurationRecorders 작업에 대한 CloudTrail 로그 파일입니다.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeDeliveryChannels

다음 예제는 DescribeDeliveryChannels 작업에 대한 CloudTrail 로그 파일입니다.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

GetResourceConfigHistory

다음 예제는 GetResourceConfigHistory 작업에 대한 CloudTrail 로그 파일입니다.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
```

```
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111111111111"
      }
```

PutConfigurationRecorder

다음 예제는 PutConfigurationRecorder 작업에 대한 CloudTrail 로그 파일입니다.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:23Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutConfigurationRecorder",
```

```
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorder": {
          "name": "default",
          "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
        }
      },
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

PutDeliveryChannel

다음 예제는 PutDeliveryChannel 작업에 대한 CloudTrail 로그 파일입니다.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
```

```
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StartConfigurationRecorder

다음 예제는 StartConfigurationRecorder 작업에 대한 CloudTrail 로그 파일입니다.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StopConfigurationRecorder

다음 예제는 StopConfigurationRecorder 작업에 대한 CloudTrail 로그 파일입니다.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

모니터링

다른 AWS 서비스를 사용하여 AWS Config 리소스를 모니터링할 수 있습니다.

- Amazon Simple Notification Service(SNS)를 사용하여 사용자 API 활동의 결과로 지원되는 AWS 리소스가 생성, 업데이트 또는 수정될 때마다 알림을 보낼 수 있습니다.
- Amazon EventBridge를 사용하여 AWS Config 이벤트의 상태 변경을 감지하고 대응할 수 있습니다.

주제

- Amazon SQS를 사용하여 AWS 리소스 변경 모니터링
- Amazon EventBridge AWS Config 를 사용한 모니터링

Amazon SQS를 사용하여 AWS 리소스 변경 모니터링

AWS Config 는 Amazon Simple Notification Service(SNS)를 사용하여 사용자 API 활동의 결과로 지원되는 AWS 리소스가 생성, 업데이트 또는 수정될 때마다 알림을 보냅니다. 하지만 사용자가 특정 리소

스 구성 변경 사항만 확인하고 싶을 때도 있습니다. 예를 들어 보안 그룹의 구성이 변경될 때는 확인할 필요가 있지만 굳이 Amazon EC2 인스턴스의 태그가 변경될 때마다 확인할 필요는 없는 경우가 여기에 해당됩니다. 또는 특정 리소스가 업데이트되면 특정 작업을 수행하는 프로그램을 개발하고자 하는 경우도 해당됩니다. 예를 들어 보안 그룹 구성이 변경되면 특정 워크플로가 시작되도록 하는 식입니다. 이러한 방법이나 다른 AWS Config 방법으로의 데이터를 프로그래밍 방식으로 사용하려면 Amazon Simple Queue Service 대기열을 Amazon SNS의 알림 엔드포인트로 사용합니다.

> **Note**
>
> Amazon SNS에서도 알림을 전송할 수 있는데, 그 형태는 이메일, SMS(단문 메시지 서비스) 수신 가능 휴대전화 및 스마트폰에 전송되는 SMS 메시지, 모바일 디바이스의 애플리케이션에 전송되는 알림 메시지, HTTP/HTTPS 엔드포인트 하나 또는 여러 개에 전송되는 알림 메시지입니다.

단일 SQS 대기열로 여러 주제를 구독할 수 있으며, 리전당 토픽이 하나이든 리전당 계정별로 토픽이 하나이든 관계없습니다. 해당 대기열로 원하는 SNS 주제를 구독해야 합니다. (여러 대기열로 SNS 주제 하나를 구독할 수 있습니다.) 자세한 내용은 Amazon SQS 대기열에 Amazon SNS 메시지 전송을 참조하세요.

Amazon SQS에 대한 권한

Amazon SQS를와 함께 사용하려면 계정에 SQS 대기열에 허용되는 모든 작업을 수행할 수 있는 권한을 부여하는 정책을 구성 AWS Config해야 합니다. 다음 예제 정책은 이름이 arn:aws:sqs:us-east-2:444455556666:queue1인 대기열의 각 구성 변경 사항과 관련된 메시지를 전송할 권한을 계정 번호 111122223333 및 계정 번호 444455556666에 부여하는 내용입니다.

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
```

```
}
```

이와 함께 SNS 주제와 이 주제를 구독하는 SQS 대기열을 연결할 권한을 부여하는 정책도 생성해야 합니다. 다음은 Amazon 리소스 이름(ARN)이 arn:aws:sns:us-east-2:111122223333:test-topic인 SNS 주제에 이름이 arn:aws:sqs:us-east-2:111122223333:test-topic-queue인 대기열에서 모든 작업을 수행할 권한을 부여하는 예시 정책입니다.

> **Note**
>
> SNS 주제와 SQS 대기열의 계정은 리전이 같아야 합니다.

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

각 정책은 여러 대기열이 아니라 단일 대기열에만 해당되는 문을 포함할 수 있습니다. Amazon SQS 정책의 기타 제한 사항에 대한 자세한 내용은 Amazon SQS 정책에 대한 특수 정보를 참조하세요.

Amazon EventBridge AWS Config 를 사용한 모니터링

Amazon EventBridge는 AWS 리소스의 변경 사항을 설명하는 시스템 이벤트의 스트림을 거의 실시간으로 제공합니다. Amazon EventBridge를 사용하여 AWS Config 이벤트 상태의 변화를 감지하고 이에 대응합니다.

상태가 달라질 때마다 또는 관심이 있는 상태로 변경될 때 실행되는 규칙을 만들면 됩니다. Amazon EventBridge는 사용자가 만든 규칙에 따라 이벤트가 규칙에 지정된 값과 일치하면 하나 이상의 대상 작업을 간접 호출합니다. 이벤트 유형에 따라 알림을 보내거나, 이벤트 정보를 캡처하거나, 교정 작업을 수행하거나, 이벤트를 시작하거나, 기타 작업을 수행할 수 있습니다.

그러나 AWS Config에 대한 이벤트 규칙을 생성하기 전에 다음을 수행해야 합니다.

- Eventbridge의 이벤트, 규칙, 대상을 숙지해야 합니다. 자세한 내용은 Amazon EventBridge란 무엇입니까?를 참조하세요.
- EventBridge 시작 및 규칙 설정 방법에 대한 자세한 내용은 Amazon EventBridge 시작하기를 참조하세요.
- 대상, 즉 이벤트 규칙에 사용할 대상을 생성합니다.

주제

- 고려 사항
- 에 대한 Amazon EventBridge 형식 AWS Config
- AWS Config용 Amazon EventBridge 규칙 생성

고려 사항

AWS Config다음 리소스 유형을 기록하지 않는 경우 EventBridge를 통해 알림을 받지 않습니다.

- `AWS::ACM::Certificate`
- `AWS::CloudTrail::Trail`
- `AWS::CloudWatch::Alarm`
- `AWS::EC2::CustomerGateway`
- `AWS::EC2::EIP`
- `AWS::EC2::Host`
- `AWS::EC2::Instance`

- AWS::EC2::InternetGateway
- AWS::EC2::NetworkAcl
- AWS::EC2::NetworkInterface
- AWS::EC2::RouteTable
- AWS::EC2::SecurityGroup
- AWS::EC2::Subnet
- AWS::EC2::VPC
- AWS::EC2::VPNConnection
- AWS::EC2::VPNGateway
- AWS::EC2::Volume
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::IAM::Group
- AWS::IAM::Policy
- AWS::IAM::Role
- AWS::IAM::User
- AWS::RDS::DBInstance
- AWS::RDS::DBSecurityGroup
- AWS::RDS::DBSnapshot
- AWS::RDS::DBSubnetGroup
- AWS::RDS::EventSubscription
- AWS::Redshift::Cluster
- AWS::Redshift::ClusterParameterGroup
- AWS::Redshift::ClusterSecurityGroup
- AWS::Redshift::ClusterSnapshot
- AWS::Redshift::ClusterSubnetGroup
- AWS::Redshift::EventSubscription
- AWS::S3::Bucket

에 대한 Amazon EventBridge 형식 AWS Config

에 대한 EventBridge 이벤트의 형식 AWS Config 은 다음과 같습니다.

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

AWS Config용 Amazon EventBridge 규칙 생성

다음 단계를 사용하여 AWS Config가 생성하는 이벤트에서 트리거되는 EventBridge 규칙을 생성합니다. 이벤트는 최선의 작업을 기반으로 발생됩니다.

1. 탐색 창에서 규칙을 선택합니다.
2. 규칙 생성을 선택합니다.
3. 규칙에 대해 이름과 설명을 입력하세요.

   규칙은 동일한 지역과 동일한 이벤트 버스의 다른 규칙과 동일한 이름을 가질 수 없습니다.

   > **Note**
   >
   > 이벤트 버스는 소스로부터 이벤트를 수신하고, 규칙을 사용하여 이벤트를 평가하고, 구성된 입력 변환을 적용하고, 적절한 대상(들)로 라우팅합니다. 계정의 기본 이벤트 버스는에서 이벤트를 수신합니다 AWS 서비스. 사용자 지정 이벤트 버스는 사용자 지정 애플리케이션 및 서비스에서 이벤트를 수신할 수 있습니다. 파트너 이벤트 버스는 SaaS 파트너가 생성한 이벤트 소스로부터 이벤트를 수신합니다. 이러한 이벤트는 파트너 서비스 또는 애플리케이션에서 발생합니다. 자세한 내용은 Amazon EventBridge 사용 설명서의 Amazon EventBridge의 이벤트 버스를 참조하세요. EventBridge

4. 규칙 유형(Rule type)에서 이벤트 패턴이 있는 규칙(Rule with an event pattern)을 생성합니다.

5. 이벤트 소스에서 AWS 이벤트 또는 EventBridge 파트너 이벤트를 선택합니다.
6. (선택 사항) 샘플 이벤트 유형에서 AWS 이벤트를 선택합니다.
7. (선택 사항) 샘플 이벤트에서 규칙을 트리거할 이벤트 유형을 선택합니다.
   - 이 서비스에 대한 API 직접 호출에 기반하는 규칙을 생성하려면 CloudTrail에서AWS API 직접 호출을 선택합니다. 이 유형의 규칙 생성에 대한 자세한 내용은 자습서: AWS CloudTrail API 호출에 대한 Amazon EventBridge 규칙 생성을 참조하세요.
   - 계정 리소스가 변경될 때 알림을 받으려면 Config Configuration Item Change(Config 구성 항목 변경)를 선택합니다.

     이러한 지원 문서에 설명된 대로 EventBridge를 사용하여 리소스가 생성되거나 삭제될 때 사용자 지정 이메일 알림을 받을 수 있습니다. AWS Config 서비스를 AWS 계정 사용하는 내에서 리소스가 생성될 때 사용자 지정 이메일 알림을 받으려면 어떻게 해야 합니까? AWS Config 서비스를 AWS 계정 사용하는 내에서 리소스가 삭제될 때 사용자 지정 이메일 알림을 받으려면 어떻게 해야 합니까?
   - 규칙에 대한 규정 준수 점검이 실패할 때 알림을 받으려면 Config Rules Compliance Change(Config 규칙 준수 변경)를 선택합니다.

     이 지원 문서에 설명된 대로 EventBridge를 사용하여 리소스가 규정을 준수하지 않을 때 사용자 지정 이메일 알림을 받을 수 있습니다.를 사용하여 AWS 리소스가 규정을 준수하지 않을 때 알림을 받으려면 어떻게 해야 하나요 AWS Config?
   - 재평가 상태 알림을 받으려면 Config Rules Re-evaluation Status(Config 규칙 재평가 상태)를 선택합니다.
   - 구성 스냅샷 전송 상태 알림을 받으려면 Config Configuration Snapshot Delivery Status(Config 구성 스냅샷 전송 상태)를 선택합니다.
   - 구성 기록 전송 상태 알림을 받으려면 Config Configuration History Delivery Status(Config 구성 내역 전송 상태)를 선택합니다.
8. 생성 방법에서 패턴 양식 사용을 선택합니다.
9. 이벤트 소스에서 AWS 서비스를 선택합니다.
10. AWS 서비스에서 Config를 선택합니다.
11. 이벤트 유형에서 규칙을 트리거할 이벤트 유형을 선택합니다.
   - 모든 서비스에 적용되는 규칙을 만들려면 모든 이벤트를 선택합니다. AWS 이 옵션을 선택할 경우 특정 메시지 유형, 규칙 이름, 리소스 유형 또는 리소스 ID를 선택할 수 없습니다.

- 이 서비스에 대한 API 직접 호출에 기반하는 규칙을 생성하려면 CloudTrail에서AWS API 직접 호출을 선택합니다. 이 유형의 규칙 생성에 대한 자세한 내용은 자습서: AWS CloudTrail API 호출에 대한 Amazon EventBridge 규칙 생성을 참조하세요.
- 계정 리소스가 변경될 때 알림을 받으려면 Config Configuration Item Change(Config 구성 항목 변경)를 선택합니다.

  이러한 지원 문서에 설명된 대로 EventBridge를 사용하여 리소스가 생성되거나 삭제될 때 사용자 지정 이메일 알림을 받을 수 있습니다. AWS Config 서비스 AWS 계정 사용 시 리소스가 생성될 때 사용자 지정 이메일 알림을 받으려면 어떻게 해야 합니까? AWS Config 서비스 AWS 계정 사용 시 리소스가 삭제될 때 사용자 지정 이메일 알림을 받으려면 어떻게 해야 합니까?
- 규칙에 대한 규정 준수 점검이 실패할 때 알림을 받으려면 Config Rules Compliance Change(Config 규칙 준수 변경)를 선택합니다.

  이 지원 문서에 설명된 대로 EventBridge를 사용하여 리소스가 규정을 준수하지 않을 때 사용자 지정 이메일 알림을 받을 수 있습니다.를 사용하여 AWS 리소스를 준수하지 않을 때 알림을 받으려면 어떻게 해야 하나요 AWS Config?
- 재평가 상태 알림을 받으려면 Config Rules Re-evaluation Status(Config 규칙 재평가 상태)를 선택합니다.
- 구성 스냅샷 전송 상태 알림을 받으려면 Config Configuration Snapshot Delivery Status(Config 구성 스냅샷 전송 상태)를 선택합니다.
- 구성 기록 전송 상태 알림을 받으려면 Config Configuration History Delivery Status(Config 구성 내역 전송 상태)를 선택합니다.

12 모든 유형의 알림을 받으려면 모든 메시지 유형을 선택합니다. 다음 유형의 알림을 받으려면 특정 메시지 유형을 선택합니다.

- ConfigurationItemChangeNotification을 선택하면가 AWS Config 평가하는 리소스의 구성이 변경되면 메시지가 수신됩니다.
- ComplianceChangeNotification을 선택할 경우 AWS Config 가 평가한 리소스의 규정 준수 유형이 변경되면 사용자가 메시지를 수신합니다.
- ConfigRulesEvaluationStarted를 선택하면가 지정된 리소스에 대해 규칙을 평가하기 AWS Config 시작할 때 메시지를 수신합니다.
- ConfigurationSnapshotDeliveryCompleted를 선택하면가 구성 스냅샷을 Amazon S3 버킷에 AWS Config 성공적으로 전송하면 메시지를 수신합니다.
- ConfigurationSnapshotDeliveryFailed를 선택하면가 구성 스냅샷을 Amazon S3 버킷으로 전송하지 AWS Config 못할 때 메시지를 수신합니다.

- ConfigurationSnapshotDeliveryStarted를 선택하면가 구성 스냅샷을 Amazon S3 버킷으로 전송하기 AWS Config 시작할 때 메시지를 수신합니다.
- ConfigurationHistoryDeliveryCompleted를 선택하면가 구성 기록을 Amazon S3 버킷에 AWS Config 성공적으로 전달하면 메시지를 수신합니다.

13. 이벤트 유형 드롭다운 목록에서 특정 이벤트 유형을 선택한 경우 모든 리소스 유형을 선택하여 AWS Config 지원되는 모든 리소스 유형에 적용되는 규칙을 만듭니다.

    또는 특정 리소스 유형을 선택한 후 AWS Config 지원 리소스 유형을 입력합니다(예: `AWS::EC2::Instance`).

14. 이벤트 유형 드롭다운 목록에서 특정 이벤트 유형을 선택한 경우, 모든 리소스 ID를 선택하여 모든 AWS Config 지원 리소스 유형 ID를 포함시킵니다.

    또는 특정 리소스 ID를 선택한 후 AWS Config 지원 리소스 ID를 입력합니다(예: `i-04606de676e635647`).

15. 이벤트 유형 드롭다운 목록에서 특정 이벤트 유형을 선택한 경우, 모든 규칙 이름을 선택하여 모든 AWS Config 지원 규칙을 포함시킵니다.

    또는 특정 규칙 이름을 선택한 후 AWS Config 지원 규칙을 입력합니다(예: required-tags).

16. 대상 유형 선택에서 이 규칙을 사용하도록 설정한 대상 유형을 선택한 후, 해당 유형에 필요한 모든 추가 옵션을 구성합니다.
17. 표시되는 필드는 선택한 서비스에 따라 달라집니다. 필요에 따라 이 대상 유형과 관련된 정보를 입력합니다.
18. 여러 대상 유형에 대해 EventBridge에서는 대상에 이벤트를 보낼 권한이 필요합니다. 이 경우 EventBridge는 규칙 실행에 필요한 IAM 역할을 생성할 수 있습니다.
    - IAM 역할을 자동으로 생성하려면 이 특정 리소스에 대해 새 역할 생성을 선택합니다.
    - 이전에 생성한 IAM 역할을 사용하려면 기존 역할 사용(Use existing role)을 선택합니다.
19. (선택 사항) 이 규칙에 다른 대상을 추가하려면 대상 추가(Add target)를 선택합니다.
20. (선택 사항)규칙에 대해 하나 이상의 태그를 입력하세요. 자세한 내용은 Amazon EventBridge 태그를 참조하세요.
21. 이벤트 모니터링 요구 사항을 충족하도록 규칙 설정을 검토하세요.
22. 생성을 선택하여 선택 사항을 확인합니다.

인터페이스 Amazon VPC 엔드포인트 AWS Config 와 함께 사용

Amazon Virtual Private Cloud(VPC)를 사용하여 AWS 리소스를 호스팅하는 경우 VPC와 간에 프라이빗 연결을 설정할 수 있습니다 AWS Config. 이 연결을 사용하면 퍼블릭 인터넷을 통하지 않고 VPC의 AWS Config 와 통신할 수 있습니다.

Amazon VPC는 사용자가 정의한 가상 네트워크에서 AWS 리소스를 시작하는 데 사용할 수 있는 AWS 서비스입니다. VPC가 있으면 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등 네트워크 설정을 제어할 수 있습니다. 인터페이스 VPC 엔드포인트는 프라이빗 IP 주소가 있는 탄력적 네트워크 인터페이스를 사용하여 AWS 서비스 간에 프라이빗 통신을 가능하게 하는 AWS 기술인 AWS PrivateLink로 구동됩니다. VPC를에 연결하려면 인터페이스 VPC 엔드포인트를 AWS Config정의합니다 AWS Config. 이러한 유형의 엔드포인트를 사용하면 VPC를 AWS 서비스에 연결할 수 있습니다. 엔드포인트는 인터넷 게이트웨이, NAT(네트워크 주소 변환) 인스턴스 또는 VPN 연결 AWS Config 없이도에 안정적이고 확장 가능한 연결을 제공합니다. 자세한 내용은 VPC 사용 설명서의 VPC란 무엇입니까? 단원을 참조하세요.

다음은 Amazon VPC 사용자를 위한 단계들입니다. 자세한 내용은 Amazon VPC 사용 설명서의 시작하기를 참조하세요.

에 대한 VPC 엔드포인트 생성 AWS Config

VPC AWS Config 에서를 사용하려면에 대한 인터페이스 VPC 엔드포인트를 생성합니다 AWS Config. 에 대한 설정을 변경할 필요가 없습니다 AWS Config.는 퍼블릭 엔드포인트를 사용하여 다른 AWS 서비스를 AWS Config 호출합니다. 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 엔드포인트 생성을 참조하세요.

FAQ

최신 구성 변경 사항을 볼 수 없습니다.

구성 변경 사항을 즉시 볼 수 있나요?

AWS Config 는 일반적으로 변경 사항이 감지된 직후 또는 지정한 빈도로 리소스에 대한 구성 변경 사항을 기록합니다. 그러나 이는 가장 이상적인 시나리오이며 경우에 따라 더 오래 걸릴 수 있습니다. 문제가 지속되면 지원에 문의하여 Amazon CloudWatch에서 지원하는 AWS Config 지표를 제공하세요. 이러한 지표에 대한 자세한 내용은 AWS Config 사용량 및 성공 지표를 참조하세요.

의 간접 관계 AWS Config

주제

- 리소스 관계란 무엇인가요?
- 리소스에 대한 직접 관계와 간접 관계는 무엇인가요?
- 가 AWS Config 지원하는 간접 관계는 무엇입니까?
- 간접 관계를 사용하는 시나리오는 무엇입니까?
- 직접 및 간접 관계로 인해 구성 항목이 어떻게 생성되나요?
- 간접 관계로 인해 생성되는 구성 항목은 무엇인가요?
- 간접 관계를 비활성화하려면 어떻게 해야 합니까?
- 간접 관계와 관련된 구성 데이터를 검색하려면 어떻게 해야 하나요?

리소스 관계란 무엇인가요?

에서 AWS리소스는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, AWS CloudFormation 스택 또는 Amazon S3 버킷과 같이 관리 가능한 엔터티를 나타냅니다. AWS Config 는 기록된 리소스 유형에 대한 변경이 감지될 때마다 또는 설정한 기록 빈도로 구성 항목(CIs)을 생성하여 리소스를 추적하고 모니터링하는 서비스입니다. 예를 들어 AWS Config 가 Amazon EC2 인스턴스를 추적하도록 설정된 경우 인스턴스가 생성, 업데이트 또는 삭제될 때마다 구성 항목을 생성합니다. 에서 생성한 각 구성 항목에 AWS Config 는 `accountId`, `arn` (Amazon 리소스 이름), , `awsRegion`, `tags`, `configuration`등 여러 필드가 있습니다`relationships`. CI의 관계 필드를 사용하면 AWS Config 가 리소스가 서로 연결되는 방식을 표시할 수 있습니다. 예를 들어, ID가 `vol-123ab45d`인 Amazon

EBS 볼륨이 ID가 `i-a1b2c3d4`인 Amazon EC2 인스턴스에 연결되고, 이 인스턴스가 보안 그룹 `sg-ef678hk`와 연결되어 있음을 나타내는 관계가 있을 수 있습니다.

리소스에 대한 직접 관계와 간접 관계는 무엇인가요?

AWS Config 는 "직접" 관계라고 하는 구성 필드에서 대부분의 리소스 유형에 대한 관계를 도출합니다. 직접 관계는 리소스 (A)와 다른 리소스 (B) 간의 단방향 연결(A→B)이며, 일반적으로 리소스 (A)의 설명 API 응답에서 얻습니다. 과거에는 AWS Config 처음에가 지원하는 일부 리소스 유형의 경우 다른 리소스의 구성에서 관계를 캡처하여 양방향(B→A)인 "간접" 관계를 생성합니다. 예를 들어, Amazon EC2 인스턴스의 해당 보안 그룹 간의 관계는 직접적입니다. Amazon EC2 인스턴스의 설명 API 응답에 보안 그룹이 포함되어 있기 때문입니다. 반면, 한 보안 그룹과 Amazon EC2 인스턴스 간의 관계는 간접적입니다. 보안 그룹을 설명해도 연결된 인스턴스에 대한 정보가 반환되지 않기 때문입니다.

예를 들어 간접 관계는 다음 질문에 답하는 데 도움이 될 수 있습니다.

- NAT 게이트웨이에 장애가 발생하면 프라이빗 서브넷의 어떤 EC2 인스턴스가 영향을 받나요?
- 라우팅 테이블이 수정된 경우 연결 문제가 발생할 수 있는 EC2 인스턴스는 무엇입니까?
- 어떤 보안 그룹이 사용된 적이 없나요?
- EC2 인스턴스에 연결된 보조 ENI는 보안 그룹과 연결되어 있습니까?

따라서 리소스 구성 변경이 감지되면는 해당 리소스에 대한 CI를 생성할 AWS Config 뿐만 아니라 간접 관계가 있는 리소스를 포함한 모든 관련 리소스에 대한 CIs도 생성합니다. 예를 들어가 Amazon EC2 인스턴스의 변경 사항을 AWS Config 감지하면 인스턴스에 대한 CI와 인스턴스와 연결된 보안 그룹에 대한 CI가 생성됩니다.

가 AWS Config 지원하는 간접 관계는 무엇입니까?

다음과 같은 간접 리소스 관계가에서 지원됩니다 AWS Config.

리소스 유형	리소스 유형과 간접적으로 관련됨		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface` ,		

리소스 유형	리소스 유형과 간접적으로 관련됨		
	AWS::EC2::Subnet , AWS::EC2::VPNGateway , AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway , AWS::EC2::CustomerGateway		

리소스 유형	리소스 유형과 간접적으로 관련됨		
AWS::EC2::Internet Gateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

간접 관계를 사용하는 시나리오는 무엇입니까?

다음은 간접 관계를 사용하는 AWS 서비스와 서비스의 기능입니다.

AWS 기능	시나리오
AWS Config 관리형 규칙	ec2-security-group-attached-to-eni 규칙은 기본이 아닌 보안 그룹이 탄력적 네트워크 인터페이스(ENI)에 연결되어 있는지 확인합니다. 간접 관계가 없으면 기본이 아닌 보안 그룹이 ENI에 연결되어 있는지 확인하기 위해 사용자 지정 규칙을 생성해야 합니다.
AWS Firewall Manager	사용 감사 보안 그룹 정책은 간접 관계를 사용하여 보안 그룹이 마지막으로 사용된 시기를 이해합니다. 간접 관계가 없으면 규칙을 트리거하지 않도록 보안 그룹을 구축하고 새 리소스에 동시에 연결해야 합니다 AWS Firewall Manager.

AWS 기능	시나리오

기본 리소스	• 기본이 아닌 VPC가 생성될 때의 기본 리소스:
	  • 기본 보안 그룹, 기본 네트워크 ACL 및 기본 라우팅 테이블.
	• 기본 VPC가 생성될 때의 기본 리소스:
	  • 기본이 아닌 VPC, 인터넷 게이트웨이 및 액세스 권한이 있는 각 가용 영역의 기본 서브넷으로 생성되는 모든 항목입니다.
	• 계정이 EC2를 처음 호출할 때 기본 VPC 생성 자체입니다.
	  • 새로 시작된 가용 영역의 계정에 대해 생성된 기본 서브넷입니다.
	
	간접 관계가 없으면 안티 엔트로피가 기본 리소스에 대한 변경 사항을 기록할 때까지 최대 12시간을 기다려야 합니다.

직접 및 간접 관계로 인해 구성 항목이 어떻게 생성되나요?

리소스 간 직접 관계(A→B)의 경우 리소스 B의 구성이 변경되면 리소스 A에 대한 구성 항목(CI)도 시작됩니다. 마찬가지로 간접 관계(B→A)의 경우 리소스 A의 구성이 변경되면 리소스 B에 대해 새 CI가 생성됩니다. 예를 들어 Amazon EC2 인스턴스와 보안 그룹이 직접 관계라면 보안 그룹의 구성이 변경되면 보안 그룹에 대한 CI와 EC2 인스턴스에 대한 CI가 생성됩니다. 마찬가지로 Amazon EC2 인스턴스와 보안 그룹이 간접 관계라면 EC2 인스턴스의 구성이 변경되면 Amazon EC2 인스턴스에 대한 CI와 보안 그룹에 대한 CI가 생성됩니다.

간접 관계로 인해 생성되는 구성 항목은 무엇인가요?

다음은 간접적인 리소스 관계로 인해 생성되는 추가 구성 항목(CI)입니다.

다음 리소스 유형에 대한 구성 변경	다음 리소스 유형에 대한 CI를 생성		
AWS::EC2::RouteTable	AWS::EC2::Instance , AWS::EC2::NetworkInterface , AWS::EC2::Subnet , AWS::EC2::VPNGateway 및 AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		

다음 리소스 유형에 대한 구성 변경	다음 리소스 유형에 대한 CI를 생성		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway , AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

간접 관계를 비활성화하려면 어떻게 해야 합니까?

간접 관계를 비활성화하려면 다음 단계를 완료하세요.

1. 계정 또는 여러 계정의 관리 계정에서 AWS Support 사례를 엽니다.
2. 지원 유형으로 기술을 선택합니다.
3. 서비스에서를 선택합니다AWS Config.
4. 범주에서 기타를 선택합니다.
5. 적절한 심각도 수준을 선택합니다.
6. 제목 줄에 간접 관계 비활성화를 입력합니다.
7. 설명에서 다음을 수행합니다.
   - 이 FAQ를 읽었으며 계속 진행하고자 하는지 확인합니다.
   - 간접 관계를 비활성화하려는 리전을 나열합니다.
   - 관리 계정에서 제출하는 경우 계정 IDs와 관련 리전을 포함합니다.

- 여러 계정의 경우 계정 IDs 및 리전이 포함된 CSV 파일을 연결할 수 있습니다.

AWS Support 엔지니어가 다음 단계와 상태 업데이트를 제공합니다. 간접 관계가 비활성화된 AWS 계정 및 리전의 목록을 유지하는 것이 좋습니다. 새 계정의 경우 새 AWS Support 사례를 제출하여 간접 관계를 비활성화합니다.

간접 관계와 관련된 구성 데이터를 검색하려면 어떻게 해야 하나요?

AWS Config 고급 쿼리에서 구조화 쿼리 언어(SQL) 쿼리를 실행하여 간접 리소스 관계와 관련된 구성 데이터를 검색할 수 있습니다. 예를 들어 특정 보안 그룹과 관련된 Amazon EC2 인스턴스의 목록을 검색하려면 다음 쿼리를 사용합니다.

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
    relationships.resourceId = 'sg-234213'
```

AWS SDKs AWS Config 사용에 대한 코드 예제

다음 코드 예제에서는 AWS 소프트웨어 개발 키트(SDK)와 AWS Config 함께를 사용하는 방법을 보여줍니다.

작업은 대규모 프로그램에서 발췌한 코드이며 컨텍스트에 맞춰 실행해야 합니다. 작업은 관련 시나리오의 컨텍스트에 따라 표시되며, 개별 서비스 함수를 직접적으로 호출하는 방법을 보여줍니다.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

코드 예시

- AWS SDKs AWS Config 사용에 대한 기본 예제
  - AWS SDKs AWS Config 를 사용하기 위한 작업
    - AWS SDK 또는 CLI와 DeleteConfigRule 함께 사용
    - CLI로 DescribeComplianceByConfigRule 사용
    - CLI로 DescribeComplianceByResource 사용
    - CLI로 DescribeConfigRuleEvaluationStatus 사용
    - AWS SDK 또는 CLI와 DescribeConfigRules 함께 사용
    - CLI로 DescribeConfigurationRecorderStatus 사용
    - CLI로 DescribeConfigurationRecorders 사용
    - CLI로 DescribeDeliveryChannels 사용
    - CLI로 GetComplianceDetailsByConfigRule 사용
    - CLI로 GetComplianceDetailsByResource 사용
    - CLI로 GetComplianceSummaryByConfigRule 사용
    - CLI로 GetComplianceSummaryByResourceType 사용
    - AWS SDK 또는 CLI와 PutConfigRule 함께 사용
    - CLI로 PutDeliveryChannel 사용

AWS SDKs AWS Config 사용에 대한 기본 예제

다음 코드 예제에서는 AWS Config SDKs에서의 기본 사항을 AWS 사용하는 방법을 보여줍니다.

예시

- AWS SDKs AWS Config 를 사용하기 위한 작업
  - AWS SDK 또는 CLI와 DeleteConfigRule 함께 사용
  - CLI로 DescribeComplianceByConfigRule 사용
  - CLI로 DescribeComplianceByResource 사용
  - CLI로 DescribeConfigRuleEvaluationStatus 사용
  - AWS SDK 또는 CLI와 DescribeConfigRules 함께 사용
  - CLI로 DescribeConfigurationRecorderStatus 사용
  - CLI로 DescribeConfigurationRecorders 사용
  - CLI로 DescribeDeliveryChannels 사용
  - CLI로 GetComplianceDetailsByConfigRule 사용
  - CLI로 GetComplianceDetailsByResource 사용
  - CLI로 GetComplianceSummaryByConfigRule 사용
  - CLI로 GetComplianceSummaryByResourceType 사용
  - AWS SDK 또는 CLI와 PutConfigRule 함께 사용
  - CLI로 PutDeliveryChannel 사용

AWS SDKs AWS Config 를 사용하기 위한 작업

다음 코드 예제에서는 AWS SDKs를 사용하여 개별 AWS Config 작업을 수행하는 방법을 보여줍니다. 각 예제에는 GitHub에 대한 링크가 포함되어 있습니다. 여기에서 코드 설정 및 실행에 대한 지침을 찾을 수 있습니다.

다음 예제에는 가장 일반적으로 사용되는 작업만 포함되어 있습니다. 전체 목록은 AWS Config API 참조를 참조하세요.

예시

- AWS SDK 또는 CLI와 DeleteConfigRule 함께 사용
- CLI로 DescribeComplianceByConfigRule 사용
- CLI로 DescribeComplianceByResource 사용
- CLI로 DescribeConfigRuleEvaluationStatus 사용
- AWS SDK 또는 CLI와 DescribeConfigRules 함께 사용
- CLI로 DescribeConfigurationRecorderStatus 사용
- CLI로 DescribeConfigurationRecorders 사용

- CLI로 DescribeDeliveryChannels 사용
- CLI로 GetComplianceDetailsByConfigRule 사용
- CLI로 GetComplianceDetailsByResource 사용
- CLI로 GetComplianceSummaryByConfigRule 사용
- CLI로 GetComplianceSummaryByResourceType 사용
- AWS SDK 또는 CLI와 PutConfigRule 함께 사용
- CLI로 PutDeliveryChannel 사용

AWS SDK 또는 CLI와 **DeleteConfigRule** 함께 사용

다음 코드 예시는 DeleteConfigRule의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS Config 규칙을 삭제하려면

다음 명령은 이름이 인 AWS Config 규칙을 삭제합니다. MyConfigRule

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- API 세부 정보는 AWS CLI 명령 참조의 DeleteConfigRule을 참조하세요.

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
```

```
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 DeleteConfigRule을 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **DescribeComplianceByConfigRule** 사용

다음 코드 예시는 `DescribeComplianceByConfigRule`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS Config 규칙에 대한 규정 준수 정보를 가져오는 방법

다음 명령은 하나 이상의 AWS 리소스에서 위반한 각 AWS Config 규칙에 대한 규정 준수 정보를 반환합니다.

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

출력에서 각 CappedCount 속성의 값은 관련 규칙을 준수하지 않는 리소스 수를 나타냅니다. 예를 들어 다음 출력은 3개의 리소스가 InstanceTypesAreT2micro라는 규칙을 준수하지 않음을 나타냅니다.

출력:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeComplianceByConfigRule 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제는 규칙에 대한 현재 평가 결과가 없으므로 INSUFFICIENT_DATA를 반환하는 규칙 ebs-optimized-instance에 대한 규정 준수 세부 정보를 검색합니다.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

출력:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

예제 2: 이 예제는 규칙 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK에 대한 비준수 리소스 수를 반환합니다.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

출력:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- API 세부 정보는 Cmdlet 참조(V4)의 DescribeComplianceByConfigRule을 참조하세요. AWS Tools for PowerShell

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **DescribeComplianceByResource** 사용

다음 코드 예시는 DescribeComplianceByResource의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS 리소스에 대한 규정 준수 정보를 가져오는 방법

다음 명령은 AWS Config에 의해 기록되고 하나 이상의 규칙을 위반하는 각 EC2 인스턴스에 대한 규정 준수 정보를 반환합니다.

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

출력에서 각 `CappedCount` 속성의 값은 리소스가 위반한 규칙의 수를 나타냅니다. 예를 들어 다음 출력은 인스턴스 `i-1a2b3c4d`가 2개의 규칙을 위반함을 나타냅니다.

출력:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
```

```
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeComplianceByResource 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제에서는 **`AWS::SSM::ManagedInstanceInventory`** 리소스 유형에 'COMPLIANT' 규정 준수 유형이 있는지 확인합니다.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

출력:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- API 세부 정보는 Cmdlet 참조(V4)의 DescribeComplianceByResource를 참조하세요. AWS Tools for PowerShell

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **`DescribeConfigRuleEvaluationStatus`** 사용

다음 코드 예시는 `DescribeConfigRuleEvaluationStatus`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS Config 규칙의 상태 정보를 가져오는 방법

다음 명령은 이름이 인 AWS Config 규칙의 상태 정보를 반환합니다. `MyConfigRule`

```
aws configservice describe-config-rule-evaluation-status --config-rule-
names MyConfigRule
```

출력:

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeConfigRuleEvaluationStatus 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 샘플은 제공된 구성 규칙에 대한 상태 정보를 반환합니다.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

출력:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
```

```
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- API 세부 정보는 Cmdlet 참조(V4)의 DescribeConfigRuleEvaluationStatus를 참조하세요. AWS Tools for PowerShell

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **DescribeConfigRules** 함께 사용

다음 코드 예시는 DescribeConfigRules의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS Config 규칙에 대한 세부 정보를 가져오는 방법

다음 명령은 이름이 인 AWS Config 규칙에 대한 세부 정보를 반환합니다. InstanceTypesAreT2micro

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

출력:

```
{
```

```
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeConfigRules를 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 샘플에는 선택한 속성과 함께 계정에 대한 구성 규칙이 나열되어 있습니다.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

출력:

```
ConfigRuleName                                      ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                      ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                               config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                 config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required          config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- API 세부 정보는 AWS Tools for PowerShell Cmdlet 참조(V4)의 DescribeConfigRules를 참조하세요.

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client
```

```
    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 DescribeConfigRules을 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **DescribeConfigurationRecorderStatus** 사용

다음 코드 예시는 DescribeConfigurationRecorderStatus의 사용 방법을 보여 줍니다.

CLI

AWS CLI

구성 레코더의 상태 정보를 가져오려면

다음 명령은 기본 구성 레코더의 상태를 반환합니다.

```
aws configservice describe-configuration-recorder-status
```

출력:

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeInstanceAssociationsStatus 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 샘플은 구성 레코더의 상태를 반환합니다.

```
Get-CFGConfigurationRecorderStatus
```

출력:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- API 세부 정보는 Cmdlet 참조(V4)의 DescribeConfigurationRecorderStatus를 참조하세요. AWS Tools for PowerShell

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **DescribeConfigurationRecorders** 사용

다음 코드 예시는 DescribeConfigurationRecorders의 사용 방법을 보여 줍니다.

CLI

AWS CLI

구성 레코더에 대한 세부 정보를 가져오려면

다음 명령은 기본 구성 레코더에 대한 세부 정보를 반환합니다.

```
aws configservice describe-configuration-recorders
```

출력:

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeConfigurationRecorders 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제는 구성 레코더의 세부 정보를 반환합니다.

```
Get-CFGConfigurationRecorder | Format-List
```

출력:

```
Name            : default
RecordingGroup  : Amazon.ConfigService.Model.RecordingGroup
RoleARN         : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- API 세부 정보는 Cmdlet 참조(V4)의 DescribeConfigurationRecorders를 참조하세요. AWS Tools for PowerShell

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **DescribeDeliveryChannels** 사용

다음 코드 예시는 DescribeDeliveryChannels의 사용 방법을 보여 줍니다.

CLI

AWS CLI

전송 채널에 대한 세부 정보를 가져오려면

다음 명령은 전송 채널에 대한 세부 정보를 반환합니다.

```
aws configservice describe-delivery-channels
```

출력:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 DescribeDeliveryChannels 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제는 리전의 전송 채널을 검색하고 세부 정보를 표시합니다.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

출력:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- API 세부 정보는 Cmdlet 참조(V4)의 DescribeDeliveryChannels를 참조하세요. AWS Tools for PowerShell

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **GetComplianceDetailsByConfigRule** 사용

다음 코드 예시는 `GetComplianceDetailsByConfigRule`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS Config 규칙에 대한 평가 결과를 가져오는 방법

다음 명령은 라는 AWS Config 규칙을 준수하지 않는 모든 리소스에 대한 평가 결과를 반환합니다`InstanceTypesAreT2micro`.

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

출력:

```
{
```

```
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 GetComplianceDetailsByConfigRule 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제는 규칙 access-keys-rotated에 대한 평가 결과를 얻고 규정 준수 유형별로 그룹화된 출력을 반환합니다.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

출력:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

예제 2: 이 예제는 COMPLIANT 리소스에 대한 규칙 access-keys-rotated에 대한 규정 준수 세부 정보를 쿼리합니다.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

출력:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- API 세부 정보는 Cmdlet 참조(V4)의 GetComplianceDetailsByConfigRule을 참조하세요. AWS Tools for PowerShell

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **GetComplianceDetailsByResource** 사용

다음 코드 예시는 GetComplianceDetailsByResource의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS 리소스에 대한 평가 결과를 가져오는 방법

다음 명령은 EC2 인스턴스 i-1a2b3c4d가 준수하지 않는 각 규칙에 대한 평가 결과를 반환합니다.

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

출력:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
```

```
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 GetComplianceDetailsByResource 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 제공된 리소스에 대한 예제 평가 결과입니다.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

출력:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- API 세부 정보는 Cmdlet 참조(V4)의 GetComplianceDetailsByResource를 참조하세요. AWS Tools for PowerShell

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **GetComplianceSummaryByConfigRule** 사용

다음 코드 예시는 GetComplianceSummaryByConfigRule의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS Config 규칙에 대한 규정 준수 요약을 가져오는 방법

다음 명령은 규정을 준수하는 규칙의 수와 규정을 미준수하는 규칙의 수를 반환합니다.

```
aws configservice get-compliance-summary-by-config-rule
```

출력에서 각 `CappedCount` 속성의 값은 규정 준수 또는 규정 미준수 규칙의 수를 나타냅니다.

출력:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- API 세부 정보는 AWS CLI 명령 참조의 GetComplianceSummaryByConfigRule 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 샘플은 규정을 준수하지 않는 Config 규칙 수를 반환합니다.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

출력:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- API 세부 정보는 Cmdlet 참조(V4)의 GetComplianceSummaryByConfigRule을 참조하세요. AWS Tools for PowerShell

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **GetComplianceSummaryByResourceType** 사용

다음 코드 예시는 `GetComplianceSummaryByResourceType`의 사용 방법을 보여 줍니다.

CLI

AWS CLI

모든 리소스 유형에 대한 규정 준수 요약을 가져오려면

다음 명령은 규정을 준수하지 않는 AWS 리소스 수와 규정을 준수하는 리소스 수를 반환합니다.

```
aws configservice get-compliance-summary-by-resource-type
```

출력에서 각 `CappedCount` 속성의 값은 규정 준수 또는 규정 미준수 리소스 수를 나타냅니다.

출력:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
```

```
                }
            }
        }
    ]
}
```

특정 리소스 유형에 대한 규정 준수 요약을 가져오는 방법

다음 명령은 규정을 준수하지 않는 EC2 인스턴스 수와 규정을 준수하는 EC2 인스턴스 수를 반환합니다.

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

출력에서 각 CappedCount 속성의 값은 규정 준수 또는 규정 미준수 리소스 수를 나타냅니다.

출력:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- API 세부 정보는 AWS CLI 명령 참조의 GetComplianceSummaryByResourceType 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 샘플은 규정 준수 또는 규정 미준수 리소스 수를 반환하고 출력을 json으로 변환합니다.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- API 세부 정보는 Cmdlet 참조(V4)의 GetComplianceSummaryByResourceType을 참조하세요. AWS Tools for PowerShell

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

AWS SDK 또는 CLI와 **PutConfigRule** 함께 사용

다음 코드 예시는 PutConfigRule의 사용 방법을 보여 줍니다.

CLI

AWS CLI

AWS 관리형 Config 규칙을 추가하려면

다음 명령은 AWS 관리형 Config 규칙을 추가하는 JSON 코드를 제공합니다.

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

RequiredTagsForEC2Instances.json은 규칙 구성이 포함된 JSON 파일입니다.

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

ComplianceResourceTypes 속성의 경우이 JSON 코드는 범위를 AWS::EC2::Instance 유형의 리소스로 제한하므로 AWS Config는 규칙에 대해 EC2 인스턴스만 평가합니다. 규칙은 관리형 규칙이므로 Owner 속성은 AWS로 설정되고 SourceIdentifier 속성은 규칙 식별자인 REQUIRED_TAGS로 설정됩니다. InputParameters 속성의 경우 규칙에 필요한 태그 키인 CostCenter 및 Owner가 지정됩니다.

명령이 성공하면 AWS Config는 출력을 반환하지 않습니다. 규칙 구성을 확인하려면 describe-config-rules 명령을 실행하고 규칙 이름을 지정합니다.

고객 관리형 Config 규칙을 추가하는 방법

다음 명령은 고객 관리형 Config 규칙을 추가하기 위한 JSON 코드를 제공합니다.

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

InstanceTypesAreT2micro.json은 규칙 구성이 포함된 JSON 파일입니다.

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
```

```
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

`ComplianceResourceTypes` 속성의 경우이 JSON 코드는 범위를 `AWS::EC2::Instance` 유형의 리소스로 제한하므로 AWS Config는 규칙에 대해 EC2 인스턴스만 평가합니다. 이 규칙은 고객 관리형 규칙이므로 `Owner` 속성은 로 설정`CUSTOM_LAMBDA`되고 `SourceIdentifier` 속성은 AWS Lambda 함수의 ARN으로 설정됩니다. `SourceDetails` 객체가 필요합니다. `InputParameters` 속성에 지정된 파라미터는 AWS Config가 규칙을 기준으로 리소스를 평가하기 위해 Lambda 함수를 호출할 때 AWS Lambda 함수로 전달됩니다.

명령이 성공하면 AWS Config는 출력을 반환하지 않습니다. 규칙 구성을 확인하려면 describe-config-rules 명령을 실행하고 규칙 이름을 지정합니다.

- API 세부 정보는 AWS CLI 명령 참조의 PutConfigRule을 참조하세요.

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub에 더 많은 내용이 있습니다. AWS 코드 예 리포지토리에서 전체 예를 찾고 설정 및 실행하는 방법을 배워보세요.

```
class ConfigWrapper:
    """
```

```
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- API 세부 정보는 AWS SDK for Python (Boto3) API 참조의 PutConfigRule을 참조하세요.

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

CLI로 **PutDeliveryChannel** 사용

다음 코드 예시는 PutDeliveryChannel의 사용 방법을 보여 줍니다.

CLI

AWS CLI

전송 채널을 생성하려면

다음 명령은 전송 채널에 대한 설정을 JSON 코드로 제공합니다.

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

deliveryChannel.json 파일이 전송 채널 속성을 지정합니다.

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

이 예에서는 다음 속성을 설정합니다.

name - 전송 채널의 이름입니다. 기본적으로 AWS 구성은 default 새 전송 채널에 이름을 할당합니다. put-delivery-channel 명령을 사용하여 전송 채널 이름을 업데이트할 수 없습니다. 이름을 변경하는 단계는 전송 채널 이름 변경을 참조하세요.s3BucketName - AWS Config가 구성 스냅샷 및 구성 기록 파일을 전송하는 Amazon S3 버킷의 이름입니다. 다른 AWS 계정에 속하는 버킷을 지정하는 경우 해당 버킷에는 AWS Config에 액세스 권한을 부여하는 정책이 있어야 합니다. 자세한 내용을 알아보려면 Amazon S3 버킷에 대한 권한을 참조하세요.

snsTopicARN - AWS Config가 구성 변경에 대한 알림을 보내는 Amazon SNS 주제의 Amazon 리소스 이름(ARN)입니다. 다른 계정에서 주제를 선택하는 경우 주제에 AWS Config에 액세스 권한을 부여하는 정책이 있어야 합니다. 자세한 내용은 SNS 주제에 대한 권한을 참조하세요.

`configSnapshotDeliveryProperties` - Config가 구성 스냅샷을 전송하는 빈도와 주기적 AWS Config 규칙에 대한 평가를 호출하는 빈도를 설정하는 `deliveryFrequency` 속성을 포함합니다.

명령이 성공하면 AWS Config는 출력을 반환하지 않습니다. 전송 채널의 설정을 확인하려면 describe-delivery-channels 명령을 실행합니다.

- API 세부 정보는 AWS CLI 명령 참조의 PutDeliveryChannel 섹션을 참조하세요.

PowerShell

Tools for PowerShell V4

예제 1: 이 예제는 기존 전송 채널의 deliveryFrequency 속성을 변경합니다.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- API 세부 정보는 Cmdlet 참조(V4)의 PutDeliveryChannel을 참조하세요. AWS Tools for PowerShell

AWS SDK 개발자 안내서 및 코드 예제의 전체 목록은 섹션을 참조하세요AWS SDK AWS Config 에서 사용. 이 주제에는 시작하기에 대한 정보와 이전 SDK 버전에 대한 세부 정보도 포함되어 있습니다.

문서 기록

다음 표에서는 설명서의 중요한 변경 사항에 대해 설명합니다 AWS Config. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

- API 버전: 2014-11-12
- 최종 설명서 업데이트: 2025년 6월 17일

변경 사항	설명	날짜
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon Bedrock 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형을 참조하세요.	2025년 6월 17일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • cloudfront-ssl-policy-check • cognito-identity-pool-unauth-access-check • ec2-enis-source-destination-check-enabled • 전송 중 elbv2-listener-encryption-in-transit • lambda-function-xray-enabled • msk-cluster-public-access-disabled • msk-connect-connector-logging-enabled	2025년 6월 13일

	• msk-unrestricted-access-check • aurora-mysql-cluster-audit-logging • redshift-cluster-multi-az-enabled • s3express-dir-bucket-lifecycle-rules-check • ssm-automation-logging-enabled • ssm-automation-block-public-sharing	
보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 Amazon Bedrock에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한 AWS 관리형 정책을 참조하세요.	2025년 5월 27일

AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 Amazon App Integrations, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Inspector , Amazon Macie, Amazon Route 53 Profiles, Amazon OpenSearch Serverless, Amazon Simple Storage Service(Amazon S3) AWS Security Hub및 Amazon SageMaker AI 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2025년 4월 30일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 redshift-serverless-default-db-name-check 관리형 규칙을 AWS Config 지원합니다.	2025년 4월 22일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 redshift-serverless-default-admin-check 관리형 규칙을 AWS Config 지원합니다.	2025년 4월 17일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 AWS B2B Data Interchange, Amazon Bedrock, AWS Clean Rooms, AWS CodeConnections, AWS Direct Connect,, AWS Database Migration Service (AWS DMS), Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service(Amazon S3), Amazon SageMaker AI, AWS Security Hub및 AWS Systems Manager Incident Manager, AWS Systems Manager Incident Manager Contacts에 대한 추가 권한을 부여합니다 AWS Systems Manager. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2025년 4월 8일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • s3-bucket-tagged • ecr-repository-tagged • sagemaker-feature-group-tagged • sagemaker-domain-tagged • cognito-user-pool-tagged	2025년 4월 1일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • nlb-cross-zone-load-balancing-enabled • redshift-serverless-publish-logs-to-cloudwatch • rds-instance-subnet-igw-check • ec2-spot-fleet-request-ct-encryption-at-rest • redshift-serverless-workgroup-encrypted-in-transit • redshift-serverless-workgroup-no-public-access • redshift-serverless-namespace-cmk-encryption • event-data-store-cmk-encryption-enabled • ecs-task-definition-network-mode-not-host • rds-proxy-tls-encryption • nlb-logging-enabled • redshift-audit-logging-enabled • s3-lifecycle-policy-check • sagemaker-image-tagged • redshift-cluster-parameter-group-tagged • ec2-dhcp-options-tagged • sagemaker-app-image-config-tagged	2025년 3월 22일

- mariadb-publish-logs-to-cloudwatch-logs
- docdb-cluster-encrypted-in-transit
- rds-sqlserver-encrypted-in-transit
- ec2-traffic-mirror-session-tagged
- ec2-launch-template-tagged
- ec2-traffic-mirror-target-tagged
- transfer-certificate-tagged
- batch-managed-compute-env-compute-resources-tagged
- lightsail-disk-tagged
- transfer-profile-tagged
- amplify-app-tagged
- ec2-prefix-list-tagged
- amplify-branch-tagged
- transfer-agreement-tagged
- datasync-task-tagged
- transfer-workflow-tagged
- sagemaker_notebook_instance_platform_version
- ec2-traffic-mirror-filter-tagged
- aurora-mysql-cluster-audit-logging
- ssm-document-tagged
- transfer-connector-tagged

- rds-mariadb-instance-encrypted-in-transit
- iam-saml-provider-tagged
- ec2-fleet-tagged
- iam-server-certificate-tagged
- iam-oidc-provider-tagged
- alb-listener-tagged
- glb-listener-tagged
- ec2-network-insights-access-scope-tagged
- lightsail-certificate-tagged
- ec2-capacity-reservation-tagged
- ec2-transit-gateway-multicast-domain-tagged
- dms-endpoint-tagged
- ec2-carrier-gateway-tagged
- dms-replication-task-tagged
- ec2-client-vpn-endpoint-tagged
- lightsail-bucket-tagged
- ec2-network-insights-access-scope-analysis-tagged
- nlb-listener-tagged
- ec2-network-insights-path-tagged

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • docdb-cluster-encrypted-in-transit • mariadb-publish-logs-to-cloudwatch-logs • aurora-mysql-cluster-audit-logging • rds-mariadb-instance-encrypted-in-transit • rds-sqlserver-encrypted-in-transit • sagemaker-notebook-instance-platform-version • appstream-fleet-multi-az • apprunner-vpc-connector-multi-az • mq-broker-general-logging-enabled • mq-active-single-instance-broker-storage-type-efs • mq-active-broker-ldap-authentication • iottwinmaker-component-type-tagged	2025년 3월 19일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • fsx-openzfs-deployment-type-check • fsx-ontap-deployment-type-check • fsx-windows-deployment-type-check • redshift-serverless-workgroup-routes-within-vpc	2025년 3월 18일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 ec2-instance-launched-with-allowed-ami 관리형 규칙을 AWS Config 지원합니다.	2025년 3월 11일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • connect-instance-logging-enabled • ecr-repository-cmk-encryption-enabled • elbv2-predefined-security-policy-ssl-check • glue-spark-job-supported-version • guardduty-runtime-monitoring-enabled • guardduty-ecs-protection-runtime-enabled • guardduty-ec2-protection-runtime-enabled • netfw-subnet-change-protection-enabled • rds-sql-server-logs-to-cloudwatch • sqs-queue-no-public-access • transfer-connector-logging-enabled	2025년 3월 7일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 Amazon Elastic Compute Cloud(Amazon EC2)에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한 AWS 관리형 정책을 참조하세요.	2025년 3월 4일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • athena-workgroup-description • amplify-app-tagged • sagemaker-app-image-config-tagged • elasticbeanstalk-application-version-description • amplify-branch-performance-mode-enabled • athena-workgroup-engine-version-auto-upgrade • sagemaker-image-description • devicefarm-instance-profile-tagged • transfer-workflow-description • ec2-traffic-mirror-session-tagged • appstream-fleet-in-vpc • transfer-agreement-tagged • ec2-traffic-mirror-target-description • transfer-agreement-description • athena-prepared-statement-description	2025년 2월 8일

- batch-managed-compute-env-compute-resources-tagged
- codedeploy-deployment-group-auto-rollback-enabled
- batch-managed-compute-environment-using-launch-template
- ec2-prefix-list-tagged
- ec2-traffic-mirror-filter-tagged
- athena-workgroup-enforce-workgroup-configuration
- transfer-certificate-tagged
- batch-compute-environment-managed
- lightsail-disk 태그 지정
- transfer-profile-tagged
- ec2-traffic-mirror-target-tagged
- appintegrations-event-integration-tagged
- datasync-task-tagged
- batch-compute-environment-enabled
- appconfig-configuration-profile-validators-not-empty
- elasticbeanstalk-application-description
- codedeploy-deployment-group-outdated-instances-update
- ec2-launch-template-tagged

- fis-experiment-template-tagged
- ivs-channel-playback-authorization-enabled
- redshift-cluster-parameter-group-tagged
- ec2-traffic-mirror-filter-description
- appintegrations-event-integration-description
- athena-data-catalog-description
- fis-experiment-template-log-configuration-exists
- amplify-app-description
- amplify-branch-tagged
- batch-job-queue-enabled
- elasticbeanstalk-environment-description
- amplify-app-branch-auto-deletion-enabled
- appconfig-hosted-configuration-version-description
- appconfig-freeform-profile-config-storage
- datasync-task-data-verification-enabled
- apprunner-service-observability-enabled
- transfer-certificate-description
- appconfig-deployment-strategy-replicate-to-ssm

	• transfer-workflow-tagged • transfer-connector-tagged • ec2-traffic-mirror-session-description • customerprofiles-object-type-allow-profile-creation • sagemaker-image-tagged	
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon Simple Storage Service(Amazon S3) 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2025년 2월 6일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon Simple Storage Service(Amazon S3) 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2025년 1월 29일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 AWS Clean Rooms, Amazon Comprehend, Amazon Elastic Compute Cloud(Amazon EC2), AWS HealthOmics Amazon Simple Storage Service(Amazon S3) 및 Amazon Simple Email Service(Amazon SES)에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한 AWS 관리형 정책을 참조하세요.	2025년 1월 16일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • appmesh-mesh-deny-tcp-forwarding • sagemaker-model-isolation-enabled • evidently-project-description • alb-internal-scheme-check • evidently-segment-description • appconfig-environment-description • apprunner-service-in-vpc • sagemaker-domain-in-vpc • nlb-internal-scheme-check • emr-security-configuration-encryption-rest • apprunner-service-no-public-access • sagemaker-model-in-vpc • appconfig-deployment-strategy-description • evidently-launch-description • iot-authorizer-token-signing-enabled	2025년 1월 9일

AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon Elastic Compute Cloud(Amazon EC2) 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2025년 1월 9일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • batch-job-queue-tagged • iottwinmaker-sync-job-tagged • codeguruprofiler-profiling-group-tagged • ivs-recording-configuration-tagged • iottwinmaker-entity-tagged • iottwinmaker-workspace-tagged • iottwinmaker-scene-tagged • acmpca-certificate-authority-tagged • appflow-flow-tagged • iotevents-detector-model-tagged • appmesh-virtual-node-logging-file-path-exists • apprunner-vpc-connector-tagged • apprunner-service-tagged • iotwireless-fuota-task-tagged • appmesh-virtual-node-backend-defaults-tls-on • codegururreviewer-repository-association-tagged • iotevents-input-tagged	2025년 1월 8일

- appmesh-virtual-gateway-logging-file-path-exists
- batch-compute-environment-tagged
- batch-scheduling-policy-tagged
- customerprofiles-object-type-tagged
- emr-security-configuration-encryption-transit
- iotwireless-service-profile-tagged
- ivs-playback-key-pair-tagged
- cassandra-keyspace-tagged
- iotevents-alarm-model-tagged
- appconfig-application-description
- appmesh-virtual-gateway-backend-defaults-tls
- ivs-channel-tagged
- iotwireless-multicast-group-tagged

AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon Elastic Compute Cloud(Amazon EC2), Amazon Cognito AWS Elemental MediaConnect및 Amazon OpenSearch Service 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2024년 12월 19일
보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책은에 대한 추가 권한을 부여합니다 AWS Organizations. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2024년 12월 18일
AWS Config 는 서비스 연결 구성 레코더를 지원합니다.	이번 릴리스에서는가 서비스 연결 구성 레코더를 AWS Config 지원합니다. 지원되는 서비스 또는를 사용하여 서비스 연결 구성 레코더를 활성화 AWS CLI하면 레코더가 사용자를 대신하여 연결된 서비스에 필요한 리소스 유형을 기록합니다. AWS Config 콘솔 또는를 사용하여 서비스 연결 구성 레코더의 세부 정보를 볼 수 있습니다 AWS CLI. 자세한 내용은 구성 레코더 작업을 참조하세요.	2024년 11월 27일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • appconfig-application-tagged • appconfig-configuration-profile-tagged • appconfig-environment-tagged • appconfig-extension-association-tagged • appmesh-gateway-route-tagged • appmesh-mesh-tagged • appmesh-route-tagged • appmesh-virtual-gateway-tagged • appmesh-virtual-node-tagged • appmesh-virtual-router-tagged • appmesh-virtual-service-tagged • evidently-launch-tagged • evidently-project-tagged • evidently-segment-tagged • frauddetector-entity-type-tagged • frauddetector-label-tagged • frauddetector-outcome-tagged	2024년 11월 12일

- frauddetector-variable-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged

보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 AWS AppConfig, AWS CloudTrail, Amazon Connect, Amazon DataZone, Amazon DevOpsGuru, AWS Glue, Identity Store, AWS IoT, AWS IoT FleetWise, AWS IoT 무선,, Amazon Interactive Video Service(Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager AWS Payment Cryptography, Amazon Relational Database Service(Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service(Amazon S3), Amazon EventBridge Scheduler AWS Systems Manager및 Amazon VPC Lattice에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2024년 11월 8일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 cognito-user-pool-advanced-security-enabled 관리형 규칙을 AWS Config 지원합니다.	2024년 11월 6일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • active-mq-supported-version • rabbit-mq-supported-version • ec2-client-vpn-connection-log-enabled • appsync-cache-encryption-at-rest • appsync-cache-ct-encryption-in-transit • vpc-endpoint-enabled • efs-filesystem-ct-encrypted • redshift-cluster-subnet-group-multi-az • sns-topic-no-public-access • rabbit-mq-supported-version • kms-key-policy-no-public-access • rds-mysql-instance-encrypted-in-transit • rds-postgres-instance-encrypted-in-transit • rds-sql-server-logs-to-cloudwatch • ec2-launch-template-imdsv2-check	2024년 10월 21일

AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • PCI DSS 4.0 운영 모범 사례 (글로벌 리소스 유형 제외) • PCI DSS 4.0 운영 모범 사례 (글로벌 리소스 유형 포함)	2024년 9월 23일
보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 Amazon OpenSearch Service Severless, Amazon AppStream, AWS Backup, AWS CloudTrail AWS Glue,, EC2 Image Builder AWS IoT, Amazon Interactive Video Service(Amazon IVS), AWS Elemental MediaConnect, AWS Elemental MediaTail or AWS HealthOmics, 및 Amazon EventBridge 스케줄러에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config 에 대한AWS 관리형 정책을 참조하세요.	2024년 9월 16일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • ec2-resources-in-logically-air-gapped-vault • ebs-resources-in-logically-air-gapped-vault • aurora-resources-in-logically-air-gapped-vault • efs-resources-in-logically-air-gapped-vault • s3-resources-in-logically-air-gapped-vault • storagegateway-resources-in-logically-air-gapped-vault • virtualmachine-resources-in-logically-air-gapped-vault	2024년 9월 3일
AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • FedRAMP(High 파트 1) 운영 모범 사례 • FedRAMP(High 파트 2) 운영 모범 사례	2024년 8월 27일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • athena-workgroup-logging-enabled • codebuild-report-group-encrypted-at-rest • cognito-user-pool-advanced-security-enabled • datasync-task-logging-enabled • efs-automatic-backups-enabled • glue-job-logging-enabled • glue-ml-transform-encrypted-at-rest • kinesis-stream-backup-retention-check • rds-aurora-postgresql-logs-to-cloudwatch • rds-postgresql-logs-to-cloudwatch • workspaces-root-volume-encryption-enabled • workspaces-user-volume-encryption-enabled	2024년 7월 22일

보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책이 Amazon Elastic File System(Amazon EFS), Amazon Redshift 및 AWS Systems Manager for SAP에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2024년 6월 17일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • s3-bucket-level-public-access-prohibited • cloudtrail-s3-bucket-access-logging	2024년 5월 8일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 iam-external-access-analyzer-enabled 관리형 규칙을 AWS Config 지원합니다.	2024년 5월 2일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • guardduty-malware-protection-enabled • guardduty-rds-protection-enabled • guardduty-s3-protection-enabled • inspector-lambda-code-scan-enabled	2024년 4월 26일
AWS Config Amazon CloudWatch를 사용하여 사용량 분석 간소화	이번 릴리스에서는 AWS Config 데이터 사용량 모니터링을 위한 Amazon CloudWatch 지표에 청구 가능한 사용량만 표시됩니다. 즉, 및 AWS Config 콘솔로 내보내는 Amazon CloudWatch 지표 모두에 청구할 수 없는 사용량 AWS Config 이 더 이상 표시되지 않습니다. 이를 통해 Amazon CloudWatch 지표를 사용하여 AWS Config 설정 및 사용량을 검증하고 청구 가능한 사용량과 관련 비용을 연관시킬 수 있습니다. 자세한 내용은 AWS Config 사용량 및 성공 지표를 참조하세요.	2024년 4월 26일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 iam-server-certificate-expiration-check 관리형 규칙을 AWS Config 지원합니다.	2024년 4월 23일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • vpc-sg-port-restriction-check • cloudtrail-all-write-s3-data-event-check • cloudtrail-all-read-s3-data-event-check	2024년 4월 17일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • guardduty-eks-protection-audit-enabled • guardduty-eks-protection-runtime-enabled • guardduty-lambda-protection-enabled • inspector-ec2-scan-enabled • inspector-ec2-scan-enabled • inspector-lambda-code-scan-enabled • redshift-unrestricted-port-access	2024년 4월 16일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 efs-mount-target-public-accessible 관리형 규칙을 AWS Config 지원합니다.	2024년 3월 20일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • dms-neptune-iam-authorization-enabled • dms-mongo-db-authentication-enabled • dms-redis-tls-enabled • dax-tls-endpoint-encryption • eks-secrets-encrypted • kinesis-firehose-delivery-stream-encrypted • mq-cloudwatch-audit-logging-enabled • mq-cloudwatch-audit-logging-enabled • opensearch-data-node-fault-tolerance • sagemaker-endpoint-config-prod-instance-count • service-catalog-shared-within-organization • transfer-family-server-no-ftp	2024년 2월 26일

보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 Amazon Managed Service for Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon ElastiCache, Amazon FSx, AWS Glue, AWS Identity and Access Management (IAM), AWS Lambda, AWS RAM, Amazon Redshift Serverless, Amazon SageMaker AI 및 Amazon Simple Notification Service(Amazon SNS)에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2024년 2월 22일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 s3-bucket-cross-region-replication-enabled 관리형 규칙을 AWS Config 지원합니다.	2024년 2월 12일

AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 AWS AppConfig, Amazon CloudWatch Evidently, AWS Identity and Access Management (IAM), Amazon MemoryDB(MemoryDB), Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon Redshift 및 AWS Transfer Family 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2024년 2월 6일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 macie-auto-sensitive-data-discovery-check 관리형 규칙을 AWS Config 지원합니다.	2024년 1월 29일

AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 Amazon AppStream, AWS Key Management Service (AWS KMS), Amazon Relationa l Database Service(RDS), Amazon Cognito, Amazon Elastic Compute Cloud(Ama zon EC2), EC2 Image Builder, AWS Ground Station AWS Mainframe Modernization, Amazon QuickSight, Amazon Redshift 및 AWS Systems Manager 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2024년 1월 3일
계정당 리전당 최대 AWS Config 규칙 수에 대한 서비스 제한 증가	이번 릴리스에서는가 계정당 AWS 리전당 1000 AWS Config 규칙을 AWS Config 지원합니다. 이 증가는 계정당 리전당 AWS Config 관리형 규칙, AWS Config 사용자 지정 규칙, AWS Config 적합성 팩, AWS Security Hub 제어 AWS Firewall Manager , 정책 및 AWS Backup 백업 계획을 포함하여 배포된 모든 규칙의 합계에 적용됩니다. 자세한 내용은 서비스 한도 섹션을 참조하세요.	2023년 12월 19일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • s3-meets-restore-time-target • ebs-meets-restore-time-target • ec2-meets-restore-time-target • rds-meets-restore-time-target • efs-meets-restore-time-target • fsx-meets-restore-time-target • aurora-meets-restore-time-target • dynamodb-meets-restore-time-target	2023년 12월 19일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 AWS AppConfig, Amazon Managed Service for Prometheus, AWS Database Migration Service (AWS DMS), (AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon CloudWatch Logs AWS Organizations 및 Amazon Simple Storage Service(Amazon S3)에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한 AWS 관리형 정책을 참조하세요.	2023년 12월 5일
미리 보기 릴리스: 고급 쿼리용 자연어 쿼리 프로세서	이 릴리스에서는 고급 쿼리용 자연어 쿼리 프로세서를 사용할 수 있습니다. 이 프로세서는 일반 영어로 질문하고 바로 사용 가능한 쿼리 형식으로 질문을 변환할 수 있는 생성형 인공지능(생성형 AI) 기능을 사용합니다. 자연어 쿼리 프로세서를 사용하면 AWS 조직 전체에서 AWS 계정 또는를 쿼리할 수 있습니다. 자세한 내용은 고급 쿼리용 자연어 쿼리 프로세서를 참조하세요.	2023년 11월 26일

주기적 기록	이번 릴리스에서는가 정기 기록을 AWS Config 지원합니다. 주기적 기록을 통해 리소스에 대한 최신 구성 변경 사항을 고정된 기간 동안 캡처할 수 있습니다. 이제 구성 레코더의 기본 빈도를 일일로 설정할 수 있습니다. 일일 기록을 사용하면 이전에 기록된 CI와 다른 경우에만 지난 24시간 동안의 리소스 최신 상태를 나타내는 구성 항목(CI)을 받을 수 있습니다. 또한 AWS Config 콘솔에는 특정 리소스 유형에 대한 기록 빈도를 재정의하거나 특정 리소스 유형을 기록에서 제외할 수 있는 새로운 기록 전략 환경이 도입되었습니다. 이렇게 하면 설정을 세부적인 요구 사항에 맞출 수 있습니다. 다음 데이터 형식이 추가되었습니다. • RecordingMode • RecordingModeOverride 다음 데이터 형식이 업데이트되었습니다. • PutConfigurationRecorder • ConfigurationRecorder • BaseConfigurationItem • ConfigurationItem	2023년 11월 26일

개발자 안내서에서 다음 페이지가 업데이트되었습니다.

- AWS 리소스 재코딩
- AWS Config 콘솔 AWS Config 설정 | 원클릭 설정
- AWS Config 콘솔로 설정 AWS Config | 수동 설정
- AWS CLI를 사용하여 설정 AWS Config

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 Amazon Cognito, Amazon Connect, Amazon EMR, AWS Ground Station, AWS Mainframe Modernization, Amazon MemoryDB, AWS Organizations, Amazon QuickSight, Amazon Relational Database Service(RDS), Amazon Redshift, Amazon Route 53 AWS Service Catalog및에 대한 추가 권한을 부여합니다 AWS Transfer Family. 또한 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` , `AWSConfigSLRApiGatewayStatementID` 및 `AWSConfigServiceRolePolicy` 정책에 대한 보안 식별자(SID)를 추가합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2023년 11월 17일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • acm-pca-root-ca-disabled • dynamodb-table-deletion-protection-enabled • ec2-client-vpn-connection-log-enabled • eks-cluster-log-enabled • emr-block-public-access • fsx-windows-audit-log-configured • fsx-openzfs-copy-tags-enabled • fsx-lustre-copy-tags-to-backups • msk-enhanced-monitoring-enabled • mq-auto-minor-version-upgrade-enabled • neptune-cluster-multi-az-enabled • opensearch-update-check • s3-access-point-in-vpc-only • s3-access-point-public-access-blocks • s3-bucket-mfa-delete-enabled	2023년 11월 9일

AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 AWS Identity and Access Managemen t (IAM), AWS Network Manager, AWS Private Certificate Authority (AWS Private CA), AWS App Mesh Amazon Connect, Amazon Elastic Compute Cloud(Ama zon EC2), Amazon Elastic Container Service(Amazon ECS), AWS IoT AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka Connect(Amazon MSK Connect), AWS Lambda및 AWS 리소스 탐색기 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 단원을 참조하세요.	2023년 11월 3일
AWS Config 는 새 적합성 팩을 지원합니다.	이번 릴리스에서는 다음 적합성 팩을 AWS Config 업데이트합니다. BNM RMiT 운영 모범 사례	2023년 10월 26일

집계자용 규정 준수 및 인벤토리 대시보드	이번 릴리스에서는 규정 준수 대시보드 페이지와 인벤토리 대시보드 페이지를 AWS Config 콘솔의 집계된 보기에 AWS Config 추가합니다. 규정 준수 대시보드 페이지의 경우 미준수 리소스 기준 상위 10개 리소스 유형, 미준수 규칙 기준 상위 10개 계정 수준 적합성 팩 등 집계자 내에서 리소스 규정 준수에 대한 인사이트를 요약하는 위젯이 포함된 자동 대시보드를 볼 수 있습니다. 인벤토리 대시보드 페이지의 경우 리소스 수 기준 상위 10개 리소스 유형, 리소스 수 기준 상위 10개 계정 등 집계자 내에서 리소스 구성 데이터에 대한 인사이트를 요약하는 위젯이 포함된 자동 대시보드를 볼 수 있습니다. 그래프 및 차트에 대한 자세한 내용은 규정 준수 대시보드 및 인벤토리 대시보드를 참조하세요.	2023년 10월 23일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 AWS Private CA, AWS App Mesh, Amazon Connect, Amazon Elastic Container Service(Amazon ECS), Amazon CloudWatch Evidently, Amazon Managed Grafana, Amazon GuardDuty, Amazon Inspector, AWS IoT, AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka(Amazon MSK), AWS Lambda AWS Network Manager, AWS Organizations 및 Amazon SageMaker AI에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2023년 10월 4일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새로운 AWS IoT, AWS IoT TwinMaker, AWS IoT 무선, Personalize Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon SageMaker AI, AWS CodeBuild, Amazon AppStream 및 Amazon Inspector 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2023년 10월 4일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • docdb-cluster-deletion-protection-enabled • docdb-cluster-audit-logging-enabled • docdb-cluster-snapshot-public-prohibited • mq-active-deployment-mode • mq-rabbit-deployment-mode • dms-auto-minor-version-upgrade-check • dms-replication-task-target db-logging • dms-replication-task-source db-logging • dms-endpoint-ssl-configured • custom-eventbus-policy-attached • global-endpoint-event-replication-enabled • route53-query-logging-enabled • rds-aurora-mysql-audit-logging-enabled • rds-cluster-auto-minor-version-upgrade-enable • appsync-authorization-check • netfw-deletion-protection-enabled	2023년 9월 21일

	• wafv2-rulegroup-logging-enabled • msk-in-cluster-node-require-tls	
AWS Config 는 새 적합성 팩을 지원합니다.	이번 릴리스에서는 다음 적합성 팩을 AWS Config 업데이트합니다. • Amazon S3 운영 모범 사례 • EC2 운영 모범 사례	2023년 9월 8일
보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책은 이제 AWS Systems Manager (Systems Manager)에 대한 권한을 제거합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2023년 9월 6일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon CodeGuru Profiler, AWS Elemental MediaConnect, AWS Transfer Family, Amazon Managed Service for Prometheus AWS Batch AWS Cloud Map및 Amazon Route 53 Resolver 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2023년 9월 6일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • athena-workgroup-encrypted-at-rest • neptune-cluster-iam-database-authentication • neptune-cluster-copy-tags-to-snapshot-enabled • neptune-cluster-cloudwatch-log-export-enabled • neptune-cluster-deletion-protection-enabled • neptune-cluster-snapshot-encrypted • neptune-cluster-backup-retention-check • neptune-cluster-encrypted • neptune-cluster-snapshot-public-prohibited • docdb-cluster-backup-retention-check • docdb-cluster-encrypted • rds-cluster-encrypted-at-rest	2023년 8월 10일

AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 AWS Amplify, Amazon AppIntegrations, AWS App Mesh Amazon Athena, Amazon Elastic Compute Cloud(Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, AWS IoT Greengrass Version 2, AWS Ground Station, AWS Elemental MediaConvert AWS Elemental MediaTailor,, Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon Personalize, Amazon Pinpoint 및 AWS Resilience Hub 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2023년 8월 3일

보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 Amazon Managed Workflows for AWS App Mesh, Amazon AppStream 2.0, AWS CloudFormation, Amazon CloudFront AWS CodeArtifact, AWS CodeBuild, Amazon Connect AWS Glue, Amazon GuardDuty, AWS Identity and Access Management (IAM), Amazon Inspector, AWS IoT, AWS IoT TwinMaker AWS IoT 무선, Amazon Managed Streaming for Apache Kafka, Amazon Macie, AWS Elemental MediaConnect, AWS Network Manager, AWS Organizations, AWS 리소스 탐색기, Amazon Route 53, Amazon Simple Storage Service(Amazon S3), Amazon Simple Notification Service(Amazon SNS) 및 Amazon EC2 Systems Manager(SSM)에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2023년 7월 28일

AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 Amazon Kinesis, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Pinpoint, Amazon Simple Storage Service(Amazon S3), Amazon Virtual Private Cloud(Amazon VPC), Amazon Kendra, Amazon Connect AWS CloudFormation, AWS AppConfig AWS App Mesh AWS App Runner, 및 AWS Database Migration Service (AWS DMS) 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2023년 7월 10일
조직 적합성 팩에 대한 서비스 한도 증가	이번 릴리스에서는가 모든 적합성 팩에서 계정당 리전당 350 AWS Config 규칙과 조직당 350개의 조직 AWS Config 규칙을 AWS Config 지원합니다. 자세한 내용은 서비스 한도 섹션을 참조하세요.	2023년 6월 13일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제에 대한 Amazon Managed Workflows에 대한 추가 권한을 부여합니다 AWS Amplify. Amazon Connect AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena, AWS Batch, AWS CloudFormation, AWS CloudTrail AWS CodeArtifact,, Amazon CodeGuru, AWS Directory Service, Amazon DynamoDB, Amazon Elastic Compute Cloud(Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, AWS Organizations, AWS IoT Greengrass, AWS Ground Station, AWS Identity and Access Management (IAM), Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon Lightsail, Amazon CloudWatch Logs, AWS Elemental MediaConnect, AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud(Amazon VPC), Personalize, Amazon QuickSight AWS Migration Hub Refactor Spaces, Amazon Simple Storage Service(Amazon S3), Amazon SageMaker AI, 및	2023년 6월 13일

AWS Transfer Family. 자세한 내용은 AWS Config에 대한 AWS 관리형 정책을 참조하세요.

AWS Config 리소스 유형별 레코딩 제외	이번 릴리스에서는를 AWS Config 사용하여 인벤토리 추적 및 규정 준수 모니터링에서 특정 유형의 AWS 리소스를 제외하는 동시에 향후 추가될 리소스를 AWS Config포함하여 현재 사용 가능한 다른 모든 지원되는 리소스 유형을 추적할 수 있습니다. 이 기능을 사용하면 규정 준수 및 거버넌스 표준이 적용되는 중요 리소스에 집중할 수 있습니다. 구성 레코더 및 기록 그룹에 대한 API 업데이트는 이전 버전과 호환됩니다. 즉, 이전 버전의 PutConfigurationRecorder API에서도 작동합니다. 업데이트된 API 또는 새 API를 사용하지 않고도 이전과 똑같은 방식으로 기록되는 리소스 유형을 계속 관리할 수 있습니다. 다음 데이터 형식이 추가되었습니다. • RecordingStrategy • ExclusionByResourceTypes 다음 데이터 형식이 업데이트되었습니다. • PutConfigurationRecorder • ConfigurationRecorder • RecordingGroup	2023년 6월 9일

	개발자 안내서에서 다음 페이지가 업데이트되었습니다. • 기록할 리소스 선택	
AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 Amazon Elastic Container Service(Amazon ECS), Amazon Keyspaces (Apache Cassandra용) (Amazon Keyspaces), AWS Signer, AWS Amplify, AWS App Mesh, AWS App Runner, Amazon AppStream 2.0 AWS CodeArtifact, Amazon Elastic Compute Cloud(Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, AWS Identity and Access Management (IAM), Amazon Pinpoint, Amazon SageMaker AI AWS Transfer Family, Amazon Data Firehose 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 단원을 참조하세요.	2023년 6월 5일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • cloudfront-s3-origin-access-control-enabled • custom-schema-registry-policy-attached • ec2-client-vpn-not-authorize-all • elasticache-supported-engine-version • macie-status-check • mq-automatic-minor-version-upgrade-enabled • mq-cloudwatch-audit-logging-enabled • netfw-logging-enabled • opensearch-encrypted-at-res • step-functions-state-machine-logging-enabled	2023년 5월 10일

AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 Amazon Route 53 Resolver, Amazon Elastic Compute Cloud(Amazon EC2), AWS IoT Wireless, AWS Network Manager, AWS Device Farm AWS Ground Station, Amazon AppFlow, Amazon Redshift, Amazon Pinpoint, AWS IoT AWS AppConfig, EC2 Image Builder, Amazon CloudWatch, AWS Panorama Amazon SageMaker 런타임, Amazon ECR 및 AWS Audit Manager 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 단원을 참조하세요.	2023년 5월 5일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여에 대한 구성 변경을 기록할 수 있습니다`AWS::NetworkFirewall::TLSInspectionConfiguration` . 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2023년 5월 1일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 Amazon Managed Workflows for AWS Amplify, AWS App Mesh AWS App Runner,,, Amazon CloudFront, AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, AWS Transfer Family Amazon Pinpoint, AWS Migration Hub, AWS Resilience Hub, Amazon CloudWatch, AWS Directory Service 및에 대한 추가 권한을 부여합니다 AWS WAF. 자세한 내용은 AWS Config에 대한 AWS 관리형 정책을 참조하세요.	2023년 4월 13일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • elasticache-auto-minor-version-upgrade-check • elasticache-repl-grp-auto-failover-enabled • elasticache-repl-grp-encrypted-at-rest • elasticache-repl-grp-encrypted-in-transit • elasticache-repl-grp-redis-auth-enabled • elasticache-subnet-group-check • cloudfront-s3-origin-non-existent-bucket	2023년 4월 10일
조직 적합성 팩에 대한 서비스 한도 증가	이 릴리스에서는 모든 조직 적합성 팩에서 계정당 350 AWS Config 규칙을 AWS Config 지원합니다. 자세한 내용은 서비스 한도 섹션을 참조하세요.	2023년 4월 3일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • acm-certificate-rsa-check • appsync-associated-with-waf • appsync-logging-enabled • elasticache-rbac-auth-enabled • mq-no-public-access • netfw-multi-az-enabled • ses-malware-scanning-enabled • eks-cluster-logging-enabled • appsync-cache-encryption-at-rest	2023년 4월 3일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새로운 Amazon AppStream 2.0, AWS Auto Scaling, Amazon Connect Amazon Elastic Compute Cloud, Amazon EventBridge, HealthLake, Kinesis 비디오 스트림, AWS IoT TwinMaker, Lookout for Vision, Network Manager, Amazon Pinpoint, Amazon Application Recovery Controller(ARC) 및 AWS RoboMaker 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 단원을 참조하세요.	2023년 4월 3일

보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 Amazon Managed Workflows for Amazon AppFlow, AWS App Runner,, Amazon AppStream 2.0, AWS CloudFormation, Amazon CloudFront, Amazon CloudWatch, AWS CodeArtifact AWS CodeCommit, AWS Device Farm,, Amazon Elastic Compute Cloud(Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast AWS Ground Station, AWS Identity and Access Management (IAM), AWS IoT, Amazon MemoryDB, Amazon Pinpoint, AWS Network Manager AWS Panorama,, Amazon Relational Database Service(Amazon RDS), Amazon Redshift 및 Amazon SageMaker AI에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2023년 3월 30일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 AWS Audit Manager에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한 AWS 관리형 정책을 참조하세요.	2023년 3월 3일
AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 AWS Elemental MediaPackage, Amazon EventBridge AWS IoT, (Amazon Simple Storage Service(Amazon S3), Amazon Elastic Compute Cloud(Amazon EC2), Amazon Lookout for Metrics, Amazon Lex, AWS Budgets AWS Device Farm, Amazon CodeGuru Reviewer Amazon Route 53 Resolver및 AWS RoboMaker 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2023년 3월 2일
보안 IAM 업데이트	AWS Config 이제가 `AWSConfigMultiAccountSetupPolicy` 정책에 대한 변경 사항을 추적합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2023년 2월 27일

AWS Config 리전 가용성별 리소스 범위	이번 릴리스에서는가 지원되는 각 리소스 유형에 대한 리전 정보를 AWS Config 제공합니다. 어떤 리전에서 어떤 리소스 유형이 지원되는지 자세한 내용을 보려면 리전 가용성별 리소스 적용 범위를 참조하세요.	2023년 2월 20일
AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 Amazon Interactive Video Service(Amazon IVS), Amazon Simple Storage Service(Amazon S3), AWS Glue Amazon Elastic Kubernetes Service(Amazon EKS), AWS IoT Amazon Relational Database Service(Amazon RDS) 및 Managed Service for Apache Flink 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2023년 2월 7일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 Amazon Managed Workflows for Apache Airflow, AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer, AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller(ARC), AWS Device Farm, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Pinpoint, AWS Identity and Access Management (IAM), Amazon GuardDuty 및 Amazon CloudWatch Logs에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2023년 2월 1일
보안 IAM 업데이트	보안 모범 사례로, `ConfigConformsServiceRolePolicy` 정책은 이제 `config:DescribeConfigRules` 에 대한 광범위한 리소스 수준 권한을 제거합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2023년 1월 12일

보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 Amazon Managed Service for Prometheus, AWS Audit Manager, AWS Device Farm, AWS Database Migration Service (AWS DMS), AWS Directory Service Amazon Elastic Compute Cloud(Amazon EC2), AWS Glue, AWS IoT, Amazon Lightsail, AWS Elemental MediaPackage AWS Network Manager,, Amazon QuickSight, AWS Resource Access Manager Amazon Application Recovery Controller(ARC), Amazon Simple Storage Service(Amazon S3) 및 Amazon Timestream에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2023년 1월 10일

AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 Amazon MQ, AWS AppConfig, AWS Cloud9, Amazon EventBridge 스키마, Amazon Fraud Detector, AWS IoT, AWS IoT Analytics, Amazon Lightsail, AWS Elemental MediaPackage (MediaPackage), Amazon Application Recovery Controller(ARC) AWS Resilience Hub및 AWS Transfer Family 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 단원을 참조하세요.	2023년 1월 5일
AWS Config 규칙 리소스 적용 범위	이번 릴리스에서는 늘어난 AWS Config 관리형 규칙 수에 대한 리소스 유형 적용 범위를 AWS Config 표시합니다.	2022년 12월 21일
AWS Config 규칙 검색 가능성	이 릴리스에서는가 평가 모드별 AWS Config 관리형 규칙 목록, 트리거 유형별 AWS Config 관리형 규칙 목록, 리전 가용성별 관리형 규칙 목록에 AWS Config대한 페이지를 AWS Config 지원합니다.	2022년 12월 21일

AWS Config 는 새 적합성 팩을 지원합니다.	이번 릴리스에서는 다음 적합성 팩을 AWS Config 업데이트합니다. • K-ISMS 운영 모범 사례 • NIST 800 171 운영 모범 사례 • PCI DSS 3.2.1 운영 모범 사례 • Esquema Nacional de Seguridad(ENS) High 운영 모범 사례 • Esquema Nacional de Seguridad(ENS) Medium 운영 모범 사례 • Esquema Nacional de Seguridad(ENS) Low 운영 모범 사례 • NZISM 운영 모범 사례 • NIST 800-53 rev 5 운영 모범 사례	2022년 12월 19일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • api-gwv2-access-logs-enabled • api-gwv2-authorization-type-configured • cloudfront-security-policy-check • ec2-launch-template-public-ip-disabled • elastic-beanstalk-logs-to-cloudwatch • sagemaker-notebook-instance-inside-vpc • sagemaker-notebook-instance-root-access-check • security-account-information-provided • storagegateway-resources-protected-by-backup-plan • wafv2-rulegroup-not-empty • wafv2-webacl-not-empty	2022년 12월 9일

AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 Amazon CloudWatch RUM, Amazon EventBridge, Amazon GuardDuty, Amazon Simple Email Service(Amazon SES), AWS Backup AWS DataSync 및 AWS Fault Injection Service (AWS FIS) 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 12월 9일

AWS Config 사전 예방적 규정 준수	이 릴리스에서는 리소스 프로비저닝 전에 AWS Config 규칙 준수를 사전에 확인하는 기능을 AWS Config 지원합니다. 이를 통해 리소스가 생성되거나 업데이트되기 전에 리소스의 구성 설정을 평가할 수 있습니다. AWS Config 를 사용하여 사전 프로비저닝 또는 사후 프로비저닝 등 리소스에 대한 구성 변경 사항을 추적하고 리소스가 원하는 구성과 일치하는지 확인합니다. 다음 데이터 형식이 추가되었습니다. • GetResourceEvaluationSummary • StartResourceEvaluation • ListResourceEvaluations 다음 데이터 형식이 업데이트되었습니다. • DescribeConfigRulesFilters • GetComplianceDetailsByResource • EvaluationResultQualifier • EvaluationModeConfiguration 개발자 안내서에서 다음 페이지가 업데이트되었습니다.	2022년 11월 28일

	• AWS Config 규칙의 구성 요소 • AWS Config 규칙의 평가 모드 및 트리거 유형 • AWS Config 관리형 규칙 • AWS Config 사용자 지정 규칙 • AWS Config 규칙 관리	
구성 레코더에 대한 AWS Config 구성 항목(CI)으로서의 드리프트 감지	이번 릴리스에서는가 구성 레코더의 모든 변경 사항을 AWS Config 추적하여 구성 레코더의 상태가 이전 상태와 다른지 또는 드리프트되었는지를 나타냅니다. 예를 들어, 추적 AWS Config 을 활성화한 리소스 유형에 대한 업데이트가 있는 경우, 구성 레코더를 중지 또는 시작한 경우 또는 구성 레코더를 삭제 또는 제거한 경우. `AWS::Config::ConfigurationRecorder` 리소스 유형은의 시스템 리소스 유형이며이 리소스 유형의 AWS Config 기록은 지원되는 모든 리전에서 기본적으로 활성화됩니다. `AWS::Config::ConfigurationRecorder` 리소스 유형 기록에는 추가 요금이 부과되지 않습니다. 자세한 내용은 구성 레코더의 드리프트 감지를 참조하세요.	2022년 11월 18일

AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새 AWS IoT Events, AWS Cloud Map, EC2 Image Builder, AWS DataSync, AWS Glue, Amazon Application Recovery Controller(ARC) 및 Amazon Elastic Container Registry(Amazon ECR) 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 단원을 참조하세요.	2022년 11월 8일
보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 AWS CloudFormation에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2022년 11월 7일

AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • 미국 연방수사국 형사사법정보부(CJIS) 운영 모범 사례 • Amazon SageMaker AI의 보안 모범 사례 • Amazon Elastic Container Registry 보안 모범 사례 다음 적합성 팩이 업데이트되었습니다. • MAS TRMG 운영 모범 사례 • NCSC 사이버 평가 프레임워크 운영 모범 사례 • NCSC 클라우드 보안 원칙 운영 모범 사례	2022년 10월 27일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제에 대한 추가 권한을 부여합니다 AWS Certificate Manager. Amazon Managed Workflows for Apache Airflow, AWS Amplify, AWS AppConfig, Amazon Keyspaces, Amazon CloudWatch, Amazon Connect AWS Glue DataBrew, Amazon Elastic Compute Cloud(Amazon EC2), Amazon Elastic Kubernetes Service(Amazon EKS), Amazon EventBridge, AWS Fault Injection Service, Amazon Fraud Detector, Amazon FSx, Amazon GameLift 서버, Amazon Location Service AWS IoT, Amazon Lex, Amazon Lightsail, Amazon Pinpoint, AWS OpsWorks, AWS Panorama AWS Resource Access Manager,, Amazon QuickSight, Amazon Relational Database Service(RDS), Amazon Rekognition, AWS RoboMaker AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service(Amazon S3), AWS Cloud Map, 및 AWS Security Token Service. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2022년 10월 19일

AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon Elastic Compute Cloud(Amazon EC2), Amazon Simple Email Service(Amazon SES) AWS AppConfig AWS Cloud Map및 AWS DataSync 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 10월 6일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon GuardDuty, Amazon SageMaker AI AWS AppSync AWS Cloud Map및 AWS DataSync 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 10월 4일
AWS Config 는 새 적합성 팩을 지원합니다.	이번 릴리스에서는가 SWIFT CSP 적합성 팩의 운영 모범 사례를 AWS Config 업데이트합니다.	2022년 10월 4일

AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • CMMC 2.0 레벨 1 운영 모범 사례 • CMMC 2.0 레벨 2 운영 모범 사례 다음 적합성 팩이 업데이트되었습니다. • Amazon API Gateway 운영 모범 사례 • AWS Well-Architected Framework 신뢰성 원칙을 위한 운영 모범 사례 • AWS Well-Architected Framework 보안 원칙 운영 모범 사례 • CMMC 레벨 1 운영 모범 사례 • CMMC 레벨 2 운영 모범 사례 • CMMC 레벨 3 운영 모범 사례 • CMMC 레벨 4 운영 모범 사례 • CMMC 레벨 5 운영 모범 사례 • FFIEC 운영 모범 사례 • FedRAMP(Low) 운영 모범 사례 • MAS Notice 655 운영 모범 사례	2022년 9월 30일

	• NBC TRMG 운영 모범 사례 • NIST 800 172 운영 모범 사례	
보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 AWS Glue에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2022년 9월 14일
AWS Config 는 새 적합성 팩을 지원합니다.	이번 릴리스에서는 SWIFT CSP 적합성 팩의 운영 모범 사례를 AWS Config 지원합니다.	2022년 9월 9일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 Amazon AppFlow에 대한 추가 권한을 부여합니다. Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOpsGuru, Amazon Elastic Compute Cloud(Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon EventBridge, Amazon EventBridge 스키마, Amazon FinSpace, Amazon Fraud Detector, Amazon GameLift 서버, Amazon Interactive Video Service(Amazon IVS), Amazon Managed Service for Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller(ARC), Amazon Route 53 Resolver, Amazon Simple Storage	2022년 9월 7일

Service(Amazon S3), Amazon SimpleDB Amazon Simple Email Service(Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync AWS Auto Scaling, AWS Backup, AWS Budgets,, AWS Cost Explorer, AWS Cloud9, AWS Directory Service AWS DataSync, AWS Elemental MediaPackage, AWS Glue AWS IoT,, AWS IoT Analytics , AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker , AWS Lake Formation, AWS License Manager, AWS Resilience Hub AWS Signer, 및 AWS Transfer Family. 자세한 내용은 AWS Config에 대한 AWS 관리형 정책을 참조하세요.

AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • Amazon CloudWatch 운영 모범 사례 • 독일 C5(Cloud Computing Compliance Controls Catalog) 운영 모범 사례 • IRS 1075 운영 모범 사례 다음 적합성 팩이 업데이트되었습니다. • AWS Control Tower Detective Guardrails 적합성 팩 • CISA Cyber Essentials 운영 모범 사례 • SME를 위한 ENISA 사이버 보안 가이드 운영 모범 사례 • FDA 타이틀 21 CFR 파트 11 운영 모범 사례 • FedRAMP(중급) 운영 모범 사례 • HIPAA 보안 운영 모범 사례 • NIST 개인정보보호 프레임워크 v1.0 운영 모범 사례 • NYDFS 23 운영 모범 사례 • UCB용 RBI 사이버 보안 프레임워크 운영 모범 사례 • RBI MD-ITF 운영 모범 사례	2022년 8월 31일

시작하기 AWS Config 및 사용자 지정 적합성 팩 업데이트	이번 릴리스에서는 시작하기 AWS Config 및 AWS Config 콘솔 설정 페이지를 AWS Config 업데이트하여 원클릭 설정 및 수동 설정 페이지를 소개합니다. AWS Config 또한는 적합성 팩 YAML 파일을 처음부터 생성하는 방법을 안내하는 사용자 지정 적합성 팩 페이지를 업데이트합니다.	2022년 8월 25일
AWS Systems Manager 적합성 팩과 문서(SSM 문서) 통합	이번 릴리스에서는 SSM 문서를 사용하여 적합성 팩 템플릿을 생성할 수 있습니다. SSM 문서에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 AWS Systems Manager 문서를 참조하세요. 다음 데이터 형식이 업데이트되었습니다. • PutConformancePack • ConformancePackDetail • TemplateSSMDocumentDetails 개발자 안내서에서 다음 페이지가 업데이트되었습니다. • AWS Config 콘솔을 사용하여 적합성 팩 배포 • AWS 명령줄 인터페이스를 사용하여 적합성 팩 배포	2022년 8월 24일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 Amazon Simple Email Service(Amazon SES) AWS DataSync및에 대한 추가 권한을 부여합니다 AWS Cloud Map. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2022년 8월 22일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새로운 Amazon Athena, Amazon Detective, Amazon SageMaker AI, Amazon Route 53, AWS Database Migration Service (AWS DMS), AWS Glue, AWS Key Management Service (AWS KMS) 및 Amazon Simple Email Service(Amazon SES) 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 8월 16일

AWS Config 는 새 적합성 팩을 지원합니다.	이번 릴리스에서는 다음 적합성 팩을 AWS Config 업데이트합니다. • NIST 1800 25 운영 모범 사례 • NIST 800 181 운영 모범 사례 • ABS CCIG 2.0 표준 워크로드 운영 모범 사례 • ABS CCIG 2.0 중요 워크로드 운영 모범 사례 • ACSC Essential 8 운영 모범 사례 • ACSC ISM 운영 모범 사례 • APRA CPG 234 운영 모범 사례 • CIS AWS 파운데이션 벤치마크 v1.4 레벨 1 운영 모범 사례 • CIS AWS 파운데이션 벤치마크 v1.4 레벨 2 운영 모범 사례 • BNM RMiT 운영 모범 사례 • NIST CSF 운영 모범 사례	2022년 8월 1일

적합성 팩의 규정 준수 점수	이번 릴리스에서는 적합성 팩의 규정 준수 점수를 AWS Config 도입하여 적합성 팩의 규정 준수 상태를 개괄적으로 파악할 수 있습니다. 이를 사용하여 적합성 팩의 규정 준수 수준을 식별, 조사 및 이해할 수 있습니다. 규정 준수 점수는 적합성 팩의 가능한 총 규칙-리소스 조합 수와 비교한 적합성 팩의 규정 준수 규칙-리소스 조합 수의 백분율입니다. 다음 데이터 형식이 업데이트되었습니다. • ListConformancePackComplianceScores • ConformancePackComplianceScore 개발자 안내서에서 다음 페이지가 업데이트되었습니다. • AWS Config 대시보드 보기 • 적합성 팩 대시보드에서 규정 준수 데이터 보기 • 적합성 팩 관리(API)	2022년 7월 26일

보안 IAM 업데이트	`ConfigConformsServiceRolePolicy` 정책은 이제 Amazon CloudWatch에 지표 데이터 포인트를 게시할 수 있는 권한을 부여합니다. 자세한 내용은 AWS Config에 대한 AWS 관리형 정책을 참조하세요.	2022년 7월 25일

보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 Amazon Elastic Container Service(Amazon ECS), Amazon ElastiCache, Amazon EventBridge, Amazon FSx, Amazon Managed Service for Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon QuickSight, Amazon Rekognition AWS RoboMaker, Amazon Simple Storage Service(Amazon S3), Amazon Simple Email Service(Amazon SES), AWS Amplify, AWS AppConfig, AWS AppSync, AWS Billing Conductor AWS DataSync AWS Firewall Manager, AWS Glue,,,, AWS IAM Identity Center (IAM Identity Center), EC2 Image Builder 및 Elastic Load Balancing에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2022년 7월 15일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon Elastic Compute Cloud(Amazon EC2) 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 7월 8일

AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 AWS Global Accelerator 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 7월 5일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • autoscaling-launch-template • ecs-task-definition-log-configuration • ecs-awsvpc-networking-enabled	2022년 7월 1일

AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • 캐나다 사이버 보안 센터 (CCCS) 중간 클라우드 제어 프로필 운영 모범 사례 • Gramm Leach Bliley 법 (GLBA) 운영 모범 사례 • GxP EU Annex 11 운영 모범 사례 • Amazon Elastic Kubernetes Service(Amazon EKS) 보안 모범 사례 • Amazon Relational Database Service(Amazon RDS) 보안 모범 사례 • 에 대한 보안 모범 사례 AWS Lambda 다음 적합성 팩이 업데이트되었습니다. • AI 및 ML 운영 모범 사례 • Amazon DynamoDB 운영 모범 사례 • CIS 핵심 보안 제어 v8 IG1 운영 모범 사례 • CIS 핵심 보안 제어 v8 IG2 운영 모범 사례 • CIS 핵심 보안 제어 v8 IG3 운영 모범 사례 • HIPAA 보안 운영 모범 사례 • NIST 800-53 rev 5 운영 모범 사례	2022년 6월 30일

	• NIST CSF 운영 모범 사례	
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon SageMaker AI 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 6월 29일
AWS Config 에서 새 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 새로운 Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon Route 53, Amazon WorkSpaces, AWS Batch, AWS Identity and Access Management Access Analyzer (IAM Access Analyzer), AWS Database Migration Service (AWS DMS) AWS Step Functions및 Elastic Load Balancing 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 6월 14일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • aurora-last-backup-recovery-point-created • dynamodb-last-backup-recovery-point-created • ebs-last-backup-recovery-point-created • ec2-last-backup-recovery-point-created • efs-last-backup-recovery-point-created • fsx-last-backup-recovery-point-created • rds-last-backup-recovery-point-created • s3-last-backup-recovery-point-created • storagegateway-last-backup-recovery-point-created • virtualmachine-last-backup-recovery-point-created	2022년 6월 13일

AWS Config 와 통합 AWS Security Hub	이번 릴리스에서는 AWS Config 관리형 및 사용자 지정 규칙 평가 결과를 조사 결과로 볼 수 있습니다 AWS Security Hub. Security Hub는 규칙 평가를 조사 결과로 변환하여 Amazon 리소스 이름(ARN), 생성 날짜 등 영향을 받는 리소스에 대한 추가 정보를 제공합니다. 이러한 조사 결과는 다른 Security Hub 조사 결과와 함께 볼 수 있으며, 보안 상태에 대한 포괄적인 개요를 제공합니다. 자세한 내용은 Security Hub로 규칙 평가 전송을 참조하세요.	2022년 6월 7일
보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 Amazon Athena, Amazon Detective, Amazon GuardDuty, Amazon Macie, Amazon Simple Email Service(Amazon SES), AWS Glue, AWS Resource Access Manager (AWS RAM) 및에 대한 추가 권한을 부여합니다 AWS IAM Identity Center. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2022년 5월 31일

AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • Amazon Elastic Container Service(Amazon ECS) 보안 모범 사례 • Amazon Elastic File System(Amazon EFS) 보안 모범 사례 • Amazon CloudFront 보안 모범 사례 • 에 대한 보안 모범 사례 AWS Auto Scaling • 에 대한 보안 모범 사례 AWS Network Firewall • 에 대한 보안 모범 사례 AWS Secrets Manager	2022년 5월 31일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon SageMaker AI 및 AWS Step Functions 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 5월 26일
AWS Config 에서 새 적합성 팩 지원	이번 릴리스에서는 NERC CIP BCSI 적합성 팩의 운영 모범 사례를 AWS Config 업데이트합니다.	2022년 5월 20일

AWS Config 규칙의 구성 요소	이번 릴리스에서는 규칙의 AWS Config 구성 요소를 AWS Config 소개합니다. 이 페이지에서는 규칙 정의의 구조, 규칙 메타데이터 및 규칙 개발 키트(RDK) 및 AWS Config 규칙 개발 키트 라이브러리(RDKlib)를 사용하여 Python으로 AWS Config 규칙을 작성하는 방법에 대한 모범 사례를 설명합니다.	2022년 5월 9일
조직 적합성 팩에 대한 서비스 한도 증가	이 릴리스에서는 모든 조직 적합성 팩에서 계정당 180 AWS Config 규칙을 AWS Config 지원합니다. 자세한 내용은 서비스 한도 섹션을 참조하세요.	2022년 5월 6일
AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • Amazon OpenSearch Service 보안 모범 사례 • Amazon Redshift 보안 모범 사례 • 에 대한 보안 모범 사례 AWS CloudTrail • 에 대한 보안 모범 사례 AWS CodeBuild • 에 대한 보안 모범 사례 AWS WAF	2022년 4월 29일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는가 s3-resources-protected-by-backup-plan 관리형 규칙을 AWS Config 지원합니다.	2022년 4월 11일

보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 전체 또는 지정된 AWS CloudTrail 이벤트 데이터 스토어(EDS)에 대한 정보를 가져오고, 전체 또는 지정된 AWS CloudFormation 리소스에 대한 정보를 가져오고, DynamoDB Accelerator(DAX) 파라미터 그룹 또는 서브넷 그룹의 목록을 가져오고, 액세스 중인 현재 리전의 계정에 대한 AWS Database Migration Service (AWS DMS) 복제 작업에 대한 정보를 가져오고, 지정된 유형의에 있는 모든 정책 목록을 가져올 수 AWS Organizations 있는 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2022년 4월 7일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • alb-desync-mode-check • autoscaling-capacity-rebalancing • autoscaling-launchconfig-requires-imdsv2 • autoscaling-launch-config-hop-limit • autoscaling-multiple-instance-types • clb-desync-mode-check • ecs-container-insights-enabled • ecs-fargate-latest-platform-version • netfw-policy-default-action-fragment-packets • netfw-policy-default-action-full-packets • netfw-policy-rule-group-associated • redshift-audit-logging-enabled • s3-lifecycle-policy-check • waf-regional-rule-not-empty • waf-regional-rulegroup-not-empty • waf-regional-webacl-not-empty	2022년 4월 4일

- vpc-peering-dns-resolution-check

AWS Config 사용자 지정 정책 규칙	이 릴리스에서는 Guard(AWS CloudFormation guard)를 사용하여 AWS Config 사용자 지정 정책 규칙을 생성할 수 AWS Config 있습니다https://github.com/aws-cloudformation/cloudformation-guard. Guard는 사용자 지정 규칙을 관리하기 위해 Lambda 함수를 생성할 필요 AWS Config 없이에서 적용하는 정책을 작성할 수 있는 policy-as-code 정책 언어입니다. Guard 정책을 사용하여 작성된 규칙은 AWS Config 콘솔에서 생성하거나 AWS Config 규칙 APIs. 개발자 안내서에서 다음 페이지가 업데이트되었습니다. • AWS Config 사용자 지정 규칙 • Guard를 사용하여 AWS Config 사용자 지정 규칙 생성 다음 데이터 형식이 업데이트되었습니다. • 소스 • CustomPolicyDetails • ConfigRuleEvaluationStatus • GetCustomRulePolicy • GetOrganizationCustomRulePolicy	2022년 4월 4일

	• OrganizationCustomPolicyRuleMetadata	
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon EMR SecurityConfiguration 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 3월 31일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 virtualmachine-resources-protected-by-backup-plan 관리형 규칙을 AWS Config 지원합니다.	2022년 3월 29일

AWS Config Amazon CloudWatch 지표와 통합	이번 릴리스에서는 AWS Config 가 이제 AWS Config 대시보드 페이지에서 Amazon CloudWatch를 사용한 AWS Config 사용량 및 성공 지표 추적을 지원합니다. CloudWatch 지표는 AWS 리소스에 대한 지표에 대한 경보를 검색, 그래프 작성 및 빌드하는 기능을 포함하여 시스템 성능에 대한 데이터를 제공하는 모니터링 서비스입니다. AWS Config 대시보드에서 사용량을 주도하는 트래픽 AWS Config 과 워크플로에서 발생한 장애에 대한 주요 지표를 확인할 수 있습니다. 다음 페이지가 업데이트되었습니다. • AWS Config 대시보드 보기	2022년 3월 29일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon GuardDuty Detector 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 3월 24일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • clb-multiple-az • cloudfront-no-deprecated-ssl-protocols • cloudfront-traffic-to-origin-encrypted • cloudwatch-alarm-action-enabled-check • ec2-no-amazon-key-pair • ec2-paravirtual-instance-check • ec2-token-hop-limit-check • ec2-transit-gateway-auto-vpc-attach-disabled • ecr-private-lifecycle-policy-configured • efs-access-point-enforce-root-directory • efs-access-point-enforce-user-identity • elbv2-multiple-az • kinesis-stream-encrypted • redshift-default-db-name-check • s3-event-notifications-enabled • sns-topic-message-delivery-notification-enabled • waf-global-rulegroup-not-empty	2022년 3월 23일

	• waf-global-rule-not-empty	
AWS Config 는 새 적합성 팩을 지원합니다.	이번 릴리스에서는 다음 적합성 팩을 AWS Config 업데이트합니다. • CIS 핵심 보안 제어 v8 IG1 운영 모범 사례 • CIS 핵심 보안 제어 v8 IG2 운영 모범 사례 • CIS 핵심 보안 제어 v8 IG3 운영 모범 사례 • AWS Well-Architected Framework 보안 원칙 운영 모범 사례 • Esquema Nacional de Seguridad(ENS) Low 운영 모범 사례 • Esquema Nacional de Seguridad(ENS) Medium 운영 모범 사례 • Esquema Nacional de Seguridad(ENS) High 운영 모범 사례 • MAS Notice 655 운영 모범 사례 • NIST 1800-25 운영 모범 사례	2022년 3월 16일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 AWS CloudFormation에 대한 추가 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2022년 3월 14일
AWS Config 관리형 규칙 업데이트	이번 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 업데이트합니다. • aurora-resources-protected-by-backup-plan • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	2022년 3월 10일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon Elastic Container Registry Public 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 3월 4일

AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon Elastic Compute Cloud 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 2월 28일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • codedeploy-auto-rollback-monitor-enabled • codedeploy-ec2-minimum-healthy-hosts-configured • codedeploy-lambda-allatonce-traffic-shift-disabled	2022년 2월 25일

AWS Config 업데이트의 로깅 및 모니터링	이 릴리스에서는 Amazon CloudWatch Events에 대한 참조를 대체하기 위해 Amazon EventBridge Events AWS Config 를 사용한 모니터링 페이지를 AWS Config 업데이트합니다. Amazon CloudWatch Amazon EventBridge는 이벤트를 관리하는 데 선호되는 방법입니다. CloudWatch Events와 EventBridge는 기본 서비스 및 API가 동일하지만 EventBridge가 더 많은 기능을 제공합니다. CloudWatch 또는 EventBridge에서 변경한 내용은 각 콘솔에 나타납니다. 자세한 내용은 Amazon EventBridge를 참조하세요.	2022년 2월 24일
AWS 용 SDK 페이지 AWS Config	이번 릴리스에서는 AWS SDK와 AWS Config 함께 사용 페이지를 AWS Config 소개합니다. AWS 소프트웨어 개발 키트(SDKs)는 널리 사용되는 많은 프로그래밍 언어에 사용할 수 있습니다. 각 SDK는 개발자가 선호하는 언어로 애플리케이션을 쉽게 구축할 수 있도록 하는 API, 코드 예시 및 설명서를 제공합니다.	2022년 2월 24일

보안 IAM 역할 신뢰 정책 업데이트	이번 릴리스에서는 및`sourceARN` /또는 (AWS STS) 작업에 `sourceAccountId` 대한 AWS Security Token Service 액세스를 제한하는 보안 보호를 신뢰 정책에 포함하도록 IAM 신뢰 정책 설명을 AWS Config 업데이트합니다. 이렇게 하면 IAM 역할 신뢰 정책이 예상 사용자 및 시나리오를 대신하여 리소스에 액세스하고 있는지 확인하는 데 도움이 됩니다. 다음 페이지가 업데이트되었습니다. • 역할에 IAM 신뢰 정책 추가	2022년 2월 18일

글로벌 리소스 유형 기록 변경 사항	AWS Config 이제는 새로운 글로벌 리소스 유형이 AWS Config 레코딩에 기록되는 방식을 변경합니다. 글로벌 리소스 유형은 생성 시 리전을 지정할 필요가 없는 AWS 리소스입니다. 이 변경 전에는 AWS Config가 지원하는 모든 리전에서 글로벌 리소스 유형의 기록을 활성화할 수 있었습니다. 이 변경 후 AWS Config 녹음에 온보딩된 새 글로벌 리소스 유형은 상용 파티션의 경우 서비스의 홈 리전에, AWS GovCloud (US) 파티션의 경우 AWS GovCloud(미국 서부)에만 기록할 수 있습니다. 이러한 새 글로벌 리소스 유형에 대한 구성 항목은 해당 홈 리전 및 AWS GovCloud(미국 서부)에서만 볼 수 있습니다. 2022년 2월 후에 온보딩된 글로벌 리소스 유형의 홈 리전 목록은 지원되는 모든 리소스 유형 기록 페이지의 표를 참조하세요.	2022년 2월 18일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 Elastic Beanstalk 환경에 대한 세부 정보 및 지정된 Elastic Beanstalk 구성 세트의 설정에 대한 설명을 가져오고, OpenSearch 또는 Elasticsearch 버전의 맵을 가져오고, 데이터베이스에 사용할 수 있는 Amazon RDS 옵션 그룹을 설명하고, CodeDeploy 배포 구성에 대한 정보를 가져올 수 있는 권한을 부여합니다. 또한이 정책은에 연결된 지정된 대체 연락처를 검색하고 AWS 계정, AWS Organizations 정책에 대한 정보를 검색하고, Amazon ECR 리포지토리 정책을 검색하고, 아카이브된 AWS Config 규칙에 대한 정보를 검색하고, Amazon ECS 태스크 정의 패밀리 목록을 검색하고, 지정된 하위 OUs 또는 계정의 루트 또는 상위 조직 단위(OU)를 나열하고, 지정된 대상 루트, 조직 단위 또는 계정에 연결된 정책을 나열할 수 있는 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2022년 2월 10일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • autoscaling-multiple-az • codebuild-project-artifact-encryption • codebuild-project-environment-privileged-check • codebuild-project-logging-enabled • codebuild-project-s3-logs-encrypted • ec2-security-group-attached-to-eni-periodic • ecr-private-image-scanning-enabled • ecr-private-tag-immutability-enabled • ecs-containers-nonprivileged • ecs-containers-readonly-access • ecs-no-environment-secrets • ecs-task-definition-memory-hard-limit • ecs-task-definition-nonroot-user • ecs-task-definition-pid-mode-check • eks-cluster-oldest-supported-version	2022년 2월 10일

	• eks-cluster-supported-version • lambda-vpc-multi-az-check • nacl-no-unrestricted-ssh-rdp • netfw-stateless-rule-group-not-empty • rds-cluster-default-admin-check • rds-db-security-group-not-allowed • rds-instance-default-admin-check • redshift-default-admin-check • s3-bucket-acl-prohibited • s3-version-lifecycle-policy-check • waf-global-webacl-not-empty	
보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 Amazon CloudWatch 로그 그룹 및 스트림을 생성하고 생성된 로그 스트림에 로그를 쓸 수 있는 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2022년 2월 2일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • opensearch-access-control-enabled • opensearch-audit-logging-enabled • opensearch-data-node-fault-tolerance • opensearch-encrypted-at-rest • opensearch-https-required • opensearch-in-vpc-only • opensearch-logs-to-cloudwatch • opensearch-node-to-node-encryption-check	2022년 1월 31일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 AWS CodeDeploy 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2022년 1월 5일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon SageMaker AI 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2021년 12월 20일

AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • SME를 위한 ENISA 사이버 보안 가이드 운영 모범 사례	2021년 12월 20일
AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • NIST 800 172 운영 모범 사례 • NIST 800 181 운영 모범 사례 다음 적합성 팩이 업데이트되었습니다. • K-ISMS 운영 모범 사례	2021년 11월 18일

AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • Amazon API Gateway 운영 모범 사례 • 의 운영 모범 사례 AWS Backup • CISA Cyber Essentials 운영 모범 사례 • DevOps 운영 모범 사례 • NIST 개인정보보호 프레임워크 v1.0 운영 모범 사례 다음 적합성 팩이 업데이트되었습니다. • FedRAMP(Low) 운영 모범 사례 • FedRAMP(중급) 운영 모범 사례	2021년 10월 29일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon OpenSearch Service 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2021년 10월 12일
AWS Config 는 새 적합성 팩을 지원합니다.	이번 릴리스에서는 다음 적합성 팩을 AWS Config 업데이트합니다. • MAS TRMG 운영 모범 사례	2021년 10월 12일

AWS Config 는 새 적합성 팩을 지원합니다.	이번 릴리스에서는 다음 적합성 팩을 AWS Config 업데이트합니다. • ABS CCIG 2.0 중요 워크로드 운영 모범 사례 • ABS CCIG 2.0 표준 워크로드 운영 모범 사례 • ACSC Essential 8 운영 모범 사례 • ACSC ISM 운영 모범 사례 • BNM RMiT 운영 모범 사례 • CMMC 레벨 1 운영 모범 사례 • CMMC 레벨 2 운영 모범 사례 • CMMC 레벨 3 운영 모범 사례 • CMMC 레벨 4 운영 모범 사례 • CMMC 레벨 5 운영 모범 사례 • FDA 타이틀 21 CFR 파트 11 운영 모범 사례 • FFIEC 운영 모범 사례 • MAS Notice 655 운영 모범 사례 • NBC TRMG 운영 모범 사례 • NERC CIP 운영 모범 사례 • NIST 800-53 rev 5 운영 모범 사례	2021년 9월 30일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책 이제 Amazon OpenSearch Service(OpenSearch Service) 도메인에 대한 세부 정보를 가져오고 특정 Amazon Relational Database Service(Amazon RDS) DB 파라미터 그룹에 대한 세부 파라미터 목록을 가져올 수 있는 권한을 부여합니다. 또한 이 정책은 Amazon ElastiCache 스냅샷에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2021년 9월 8일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 새 Amazon Elastic Compute Cloud 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2021년 9월 7일

AWS Config 에서 새 적합성 팩 지원	이번 릴리스에서는 다음 적합성 팩을 AWS Config 업데이트합니다. • APRA CPG 234 운영 모범 사례 • CIS AWS 파운데이션 벤치마크 v1.4 레벨 1 운영 모범 사례 • CIS AWS 파운데이션 벤치마크 v1.4 레벨 2 운영 모범 사례 • NCSC 클라우드 보안 원칙 운영 모범 사례 • NCSC 사이버 평가 프레임워크 운영 모범 사례 • NIST 800 171 운영 모범 사례 • NIST CSF 운영 모범 사례 • UCB용 RBI 사이버 보안 프레임워크 운영 모범 사례 • RBI MD-ITF 운영 모범 사례 • NYDFS 23 운영 모범 사례 • PCI DSS 3.2.1 운영 모범 사례	2021년 8월 30일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • aurora-resources-protected-by-backup-plan • backup-plan-min-frequency-and-min-retention-check • backup-recovery-point-encrypted • backup-recovery-point-manual-deletion-disabled • backup-recovery-point-minimum-retention-check • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	2021년 8월 20일
AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • NZISM 운영 모범 사례	2021년 8월 20일

보안 Amazon SNS 정책 업데이트	이번 릴리스에서는 서비스 연결 역할을 사용할 때 Amazon SNS 주제에 대한 IAM 정책 설명을 AWS Config 업데이트하여 주제 정책에 `sourceARN` 및/또는 `sourceAccountId` 를 통한 액세스를 제한하는 보안 보호를 포함합니다. 이렇게 하면 Amazon SNS가 예상 사용자 및 시나리오를 대신하여 리소스에 액세스하고 있는지 확인할 수 있습니다. 다음 페이지가 업데이트되었습니다. • Amazon SNS 주제에 대한 권한	2021년 8월 17일

보안 AWS Lambda 정책 업데이트	이번 릴리스에서는 및`sourceARN` /또는 `sourceAccountId` 호출 요청에 대한 액세스를 제한하는 보안 보호를 포함하도록 사용자 지정 규칙에 대한 AWS Lambda AWS Config 리소스 기반 정책을 AWS Config 업데이트합니다. 이렇게 하면 AWS Lambda 가 예상 사용자 및 시나리오를 대신하여 리소스에 액세스하는지 확인할 수 있습니다. 다음 페이지가 업데이트되었습니다. • AWS::Config::ConfigRule • 에 대한 사용자 지정 규칙 개발 AWS Config	2021년 8월 12일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 Amazon Kinesis 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2021년 8월 6일

AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • Esquema Nacional de Seguridad(ENS) High 운영 모범 사례 다음 적합성 팩이 업데이트되었습니다. • AWS Well-Architected Framework 신뢰성 원칙을 위한 운영 모범 사례 • AWS Well-Architected Framework 보안 원칙 운영 모범 사례 • Esquema Nacional de Seguridad(ENS) Low 운영 모범 사례 • Esquema Nacional de Seguridad(ENS) Medium 운영 모범 사례 • HIPAA 보안 운영 모범 사례	2021년 7월 30일
AWS Config 사용자 지정 규칙에 대한 AWS Lambda 함수 예제	이 릴리스에서는 AWS Config 규칙에 대한 함수 예제(Python)에 Python 예제 AWS Lambda 함수를 AWS Config 제공합니다.	2021년 7월 29일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 로그 그룹의 태그를 나열하고, 상태 시스템의 태그를 나열하고, 모든 상태 시스템을 나열할 수 있는 권한을 부여합니다. 이러한 정책은 상태 시스템에 대한 세부 정보를 가져올 수 있는 권한을 부여합니다. 이러한 정책은 이제 Amazon EC2 Systems Manager(SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka(Amazon MSK), Amazon Relational Database Service(RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notification Service AWS Database Migration Service AWS Global Accelerator및에 대한 추가 권한도 지원합니다 AWS Storage Gateway. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2021년 7월 28일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 AWS Backup 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2021년 7월 14일

AWS Config 는 새 적합성 팩을 지원합니다.	이 릴리스에서는 다음 적합성 팩을 AWS Config 지원합니다. • CIS 핵심 보안 제어 v8 IG1 운영 모범 사례 • CIS 핵심 보안 제어 v8 IG2 운영 모범 사례 • CIS 핵심 보안 제어 v8 IG3 운영 모범 사례 • NIST 1800 25 운영 모범 사례	2021년 7월 9일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • ssm-document-not-public • s3-account-level-public-access-blocks-periodic	2021년 6월 25일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • ec2-instance-multiple-eni-check • elbv2-acm-certificate-required • autoscaling-launch-config-public-ip-disabled	2021년 6월 10일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 IAM Access Analyzer에 대한 AWS Systems Manager 문서 및 정보의 권한을 볼 수 있는 권한을 부여합니다. 이러한 정책은 이제 Amazon Kinesis, Amazon ElastiCache, Amazon EMR AWS Network Firewall, Amazon Route 53 및 Amazon Relational Database Service(RDS)에 대한 추가 AWS 리소스 유형을 지원합니다. 이러한 권한 변경을 통해는 이러한 리소스 유형을 지원하는 데 필요한 읽기 전용 APIs AWS Config 호출할 수 있습니다. 이러한 정책은 이제 lambda-inside-vpc 관리형 규칙에 대한 Lambda AWS Config @Edge 함수 필터링도 지원합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2021년 6월 8일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 지원합니다. • elasticsearch-logs-to-cloudwatch • rds-cluster-multi-az-enabled • api-gw-associated-with-waf • iam-policy-no-statements-with-full-access	2021년 5월 19일

AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 Amazon Elastic File System 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2021년 5월 13일
보안 IAM 업데이트	이제 `AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은가 API Gateway AWS Config 에 대한 Config 규칙을 지원하기 위해 API Gateway에 대한 읽기 전용 GET 호출을 수행할 수 있는 권한을 부여합니다. 또한 이러한 정책은가 새 `AWS::S3::AccessPoint` 리소스 유형을 지원하는 AWS Config 데 필요한 Amazon Simple Storage Service(Amazon S3) 읽기 전용 APIs를 호출할 수 있는 권한을 추가합니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2021년 5월 10일
AWS Config 사용자 지정 규칙	개발자 안내서에서 다음 페이지가 업데이트되었습니다. • 에 대한 사용자 지정 규칙 시작하기 AWS Config • 에 대한 사용자 지정 규칙 개발 AWS Config	2021년 4월 30일

AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • aurora-mysql-backtracking-enabled • ec2-instance-profile-attached • ecs-task-definition-user-for-host-mode-check • no-unrestricted-route-to-igw • rds-automatic-minor-version-upgrade-enabled • redshift-enhanced-vpc-routing-enabled	2021년 4월 15일

보안 IAM 업데이트	`AWSConfigServiceRolePolicy` 정책 및 `AWS_ConfigRole` 정책은 이제 AWS Systems Manager 지정된 문서에 대한 정보를 볼 수 있는 권한을 부여합니다. 이러한 정책은 이제 Amazon Elastic File System AWS Backup, Amazon ElastiCache, Amazon Simple Storage Service(Amazon S3), Amazon Elastic Compute Cloud(Amazon EC2), Amazon Kinesis, Amazon SageMaker AI AWS Database Migration Service및 Amazon Route 53에 대한 추가 AWS 리소스 유형도 지원합니다. 이러한 권한 변경을 통해는 이러한 리소스 유형을 지원하는 데 필요한 읽기 전용 APIs AWS Config 호출할 수 있습니다. 자세한 내용은 AWS Config에 대한AWS 관리형 정책을 참조하세요.	2021년 4월 14일

구성 항목(CI)으로서의 적합성 팩 규정 준수	이번 릴리스에서는가 적합성 팩 규정 준수를 구성 항목으로 AWS Config 지원합니다. 이를 통해 다음과 같은 작업이 가능합니다. • 적합성 팩의 규정 준수 상태 변경 타임라인을 확인 • 여러 계정 및 리전에서 적합성 팩 규정 준수를 집계 • 고급 쿼리를 사용하여 적합성 팩의 규정 준수를 확인 다음 데이터 형식이 업데이트되었습니다. • DescribeAggregateComplianceByConformancePacks • GetAggregateConformancePackComplianceSummary 개발자 안내서에서 다음 페이지가 업데이트되었습니다. • 적합성 팩 대시보드에서 규정 준수 데이터 보기 • 적합성 팩의 규정 준수 이력 타임라인 보기 • 집계자 대시보드에서 규정 준수 데이터 보기 • AWS 리소스의 현재 구성 상태 쿼리 • 지원되는 리소스 유형	2021년 3월 30일

페이지 매김 업데이트	이번 릴리스에서는 AWS Config 고급 쿼리 기능이 이제 COUNT 및 SUM과 같은 집계 함수가 포함된 쿼리에 대한 페이지 매김을 지원합니다. 이전에는 500행으로 제한되었던 페이지 매김을 통해 이제 고급 쿼리를 사용하여 집계 쿼리의 전체 결과를 얻을 수 있습니다. 자세한 내용은 AWS 리소스의 현재 구성 상태 쿼리를 참조하세요.	2021년 3월 26일
리전 지원	이번 릴리스에서는 아시아 태평양(오사카) 리전에서 및 AWS Config AWS Config 규칙이 지원됩니다.	2021년 3월 4일
AWS Config 에서 새 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 Amazon Elastic Container Registry, Amazon Elastic Container Service 및 Amazon Elastic Kubernetes Service 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 지원되는 리소스 유형 섹션을 참조하세요.	2021년 2월 25일

KMS 암호화 지원	이번 릴리스에서는가 S3 버킷 전송을 위해 전달하는 객체에 KMS 기반 암호화 AWS Config 를 사용할 수 AWS Config 있습니다. 다음 데이터 형식이 업데이트 되었습니다. • DeliveryChannel • PutDeliveryChannel 개발자 안내서에서 다음 페이지가 업데이트되었습니다. • KMS 키에 대한 권한 • 에 할당된 IAM 역할에 대한 권한 AWS Config	2021년 2월 16일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • secretsmanager-secret-periodic-rotation • secretsmanager-secret-unused • secretsmanager-using-cmk	2021년 2월 16일
저장된 쿼리 리전 지원	이번 릴리스에서는 저장된 쿼리가 이제 AWS GovCloud(미국 동부) 및 AWS GovCloud(미국 서부) 리전에서 지원됩니다.	2021년 2월 15일

다중 계정 다중 리전 데이터 집계 영역 지원	이번 릴리스는 이제 아프리카(케이프타운) 및 유럽(밀라노) 리전에서 다중 계정 다중 리전 집계를 지원합니다. 자세한 내용은 다중 계정 다중 리전 데이터 집계를 참조하세요.	2021년 2월 15일
고급 쿼리 리전 지원	이번 릴리스는 이제 아프리카(케이프타운) 및 유럽(밀라노) 리전에서 고급 쿼리를 지원합니다. 자세한 내용은 AWS 리소스의 현재 구성 상태 쿼리를 참조하세요.	2021년 2월 15일
AWS Config RSS 피드를 통해 사용 가능한 설명서 기록 알림	이제 RSS 피드를 구독하여 AWS Config 설명서 업데이트에 대한 알림을 받을 수 있습니다.	2021년 1월 1일

이전 업데이트

다음 표에서는 2020년 12월 31일 AWS Config 이전의 설명서 릴리스 기록을 설명합니다.

변경 사항	설명	릴리스 날짜
저장된 쿼리 지원	이번 릴리스에서는 AWS Config 에서 쿼리를 저장할 수 있습니다. 저장한 쿼리는 검색하거나, 쿼리 편집기에 복사하거나, 편집하거나, 삭제할 수 있습니다. 쿼리를 저장하는 방법에 대한 자세한 내용은 용 SQL 쿼리 편집기를 사용한 쿼리 AWS Config (콘솔) 및 (AWS CLI)용 AWS Config SQL 쿼리 편집기를 사용한 쿼리 섹션을 참조하세요. API에 대한 자세한 내용은 AWS Config API 참조를 참조하세요.	2020년 12월 21일

변경 사항	설명	릴리스 날짜
	• PutStoredQuery • GetStoredQuery • ListStoredQueries • DeleteStoredQuery 에 대한 서비스 제한 AWS Config 섹션도 참조하세요.	
프로세스 확인 지원	이번 릴리스에서는 적합성 팩의 일부로 확인이 필요한 외부 및 내부 작업을 추적할 수 있는 AWS Config 규칙 유형인 프로세스 검사를 AWS Config 지원합니다. 프로세스 확인을 사용하면 요구 사항 및 조치의 준수 여부를 단일 위치에서 나열할 수 있습니다. 프로세스 확인에 대한 자세한 내용은 AWS Config 에 대한 적합성 팩 내 프로세스 검사 AWS Config 주제 및 PutExternalEvaluation API를 참조하세요.	2020년 12월 17일

변경 사항	설명	릴리스 날짜
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • api-gw-ssl-enabled • api-gw-xray-enabled • beanstalk-enhanced-health-reporting-enabled • cloudfront-accesslogs-enabled • cloudfront-associated-with-waf • cloudfront-custom-ssl-certificate • elastic-beanstalk-managed-updates-enabled • rds-cluster-iam-authentication-enabled • redshift-cluster-kms-enabled • s3-bucket-level-public-access-prohibited • subnet-auto-assign-public-ip-disabled • vpc-network-acl-unused-check	2020년 12월 17일
AWS Config 에서 지원 AWS Network Firewall	이번 릴리스에서는 AWS Config 를 사용하여 your AWS Network Firewall FirewallPolicy, RuleGroup 및 Firewall 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2020년 12월 4일

변경 사항	설명	릴리스 날짜
설명서 업데이트	AWS Config 는 위임된 관리자 계정에서 조직 전체의 리소스 데이터 집계에 대한 지원을 추가했습니다. 위임된 관리자 계정을 사용하여 AWS Organizations에서 조직 내 모든 멤버 계정의 리소스 구성 및 규정 준수 데이터를 집계할 수 있습니다. 자세한 내용은 PutConfigurationAggregator, 에 대한 집계자 생성 AWS Config 및 에 위임된 관리자 등록 AWS Config 섹션을 참조하세요.	2020년 12월 4일
AWS Config 는 새 적합성 팩을 지원합니다.	• Esquema Nacional de Seguridad (ENS) Low 운영 모범 사례 • Esquema Nacional de Seguridad (ENS) Medium 운영 모범 사례 • NCSC 사이버 평가 프레임워크 운영 모범 사례 • UCB용 RBI 사이버 보안 프레임워크 운영 모범 사례	2020년 10월 30일

변경 사항	설명	릴리스 날짜
AWS Config 는 새 적합성 팩을 지원합니다.	• ACSC Essential 8 운영 모범 사례 • ACSC ISM 운영 모범 사례 • AI 및 ML 운영 모범 사례 • 자산 관리 운영 모범 사례 • BCP 및 DR 운영 모범 사례 • EC2 운영 모범 사례 • K-ISMS 운영 모범 사례 • 로드 밸런싱 운영 모범 사례 • 로깅 운영 모범 사례 • 모니터링 운영 모범 사례 • 서버리스 운영 모범 사례	2020년 10월 22일
AWS Config 는 새 적합성 팩을 지원합니다.	• APRA CPG 234 운영 모범 사례 • FedRAMP(Low) 운영 모범 사례 • MAS Notice 655 운영 모범 사례 • NBC TRMG 운영 모범 사례 • NCSC 클라우드 보안 원칙 운영 모범 사례 • RBI MD-ITF 운영 모범 사례	2020년 10월 15일

변경 사항	설명	릴리스 날짜
AWS Config 는 새 적합성 팩을 지원합니다.	• ABS CCIG 2.0 중요 워크로드 운영 모범 사례 • ABS CCIG 2.0 표준 워크로드 운영 모범 사례 • BNM RMiT 운영 모범 사례 • 데이터 복원력 운영 모범 사례 • 데이터 레이크 및 분석 서비스 운영 모범 사례 • 암호화 및 키 관리 운영 모범 사례 • FDA 타이틀 21 CFR 파트 11 운영 모범 사례 • 공개적으로 액세스 가능한 리소스 운영 모범 사례 • MAS TRMG 운영 모범 사례 • NERC CIP BCSI 운영 모범 사례 • NYDFS 23 운영 모범 사례	2020년 10월 8일
AWS Config 는 새 적합성 팩을 지원합니다.	• AWS Well-Architected Framework 신뢰성 원칙의 운영 모범 사례 • AWS Well-Architected Framework 보안 원칙의 운영 모범 사례 • 컴퓨팅 서비스 운영 모범 사례 • 데이터베이스 서비스 운영 모범 사례 • 관리 및 거버넌스 서비스 운영 모범 사례 • 네트워킹 및 콘텐츠 전송 서비스 운영 모범 사례 • 보안, 자격 증명 및 규정 준수 서비스 운영 모범 사례 • 스토리지 서비스 운영 모범 사례	2020년 10월 26일

변경 사항	설명	릴리스 날짜
AWS Config 는 새 적합성 팩을 지원합니다.	• FedRAMP(Moderate) 운영 모범 사례 • FFIEC 운영 모범 사례 • HIPAA 보안 운영 모범 사례 • NIST 800-53 rev 4 운영 모범 사례 • NIST 800 171 운영 모범 사례	2020년 9월 28일
설명서 업데이트	다음 적합성 팩 항목이 업데이트되었습니다. • 용 적합성 팩의 사전 조건 AWS Config • 용 적합성 팩 배포 AWS Config • 조직의 모든 계정에서 AWS Config 에 대한 적합성 팩 관리	2020년 9월 28일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • iam-customer-policy-blocked-kms-actions • iam-inline-policy-blocked-kms-actions	2020년 9월 17일
AWS Config 에서 AWS WAF v2 지원	이번 릴리스에서는 AWS Config 를 사용하여 AWS WAF v2 WebACL, IPSet, RegexPatternSet, RuleGroup 및 ManagedRuleSet 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2020년 9월 1일

변경 사항	설명	릴리스 날짜
설명서 업데이트	전체 액세스 권한을 부여하는 사용자 지정 권한 생성에 대한 주의 사항이 에 대한 전체 액세스 AWS Config에 추가되었습니다. 설명서에서 다음 규칙에 대한 내용이 업데이트되었습니다. • s3-bucket-server-side-encryption-enabled • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-platform-check	2020년 8월 24일
설명서 업데이트	PCI DSS 3.2.1 운영 모범 사례 및 NIST CSF 운영 모범 사례 템플릿이 업데이트되었습니다.	2020년 8월 14일
설명서 업데이트	예제 관계 쿼리가 추가되었습니다. 자세한 내용은 AWS Config예제 관계 쿼리 섹션을 참조하세요.	2020년 7월 30일

변경 사항	설명	릴리스 날짜
설명서 업데이트	다음 데이터 형식이 업데이트되었습니다. • ConfigurationAggregator • RemediationConfiguration • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus	2020년 7월 23일
AWS Config 는 AWS Systems Manager 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 AWS Systems Manager 파일 데이터 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2020년 7월 9일
설명서 업데이트	AWS 자격 증명 및 액세스 관리를 위한 운영 모범 사례 및 PCI DSS 3.2.1 운영 모범 사례 템플릿이 업데이트되었습니다.	2020년 7월 9일

변경 사항	설명	릴리스 날짜
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • account-part-of-organizations • alb-http-drop-invalid-header-enabled • alb-waf-enabled • cloudfront-default-root-object-configured • cloudfront-origin-access-identity-enabled • cloudfront-origin-failover-enabled • cloudfront-sni-enabled • cloudtrail-security-trail-enabled • cw-loggroup-retention-period-check • dax-encryption-enabled • dynamodb-in-backup-plan • ebs-in-backup-plan • ec2-imdsv2-check • efs-in-backup-plan • eks-endpoint-no-public-access • eks-secrets-encrypted • elasticsearch-node-to-node-encryption-check • elb-cross-zone-load-balancing-enabled • elb-tls-https-listeners-only • iam-no-inline-policy-check • rds-cluster-deletion-protection-enabled	2020년 7월 9일

변경 사항	설명	릴리스 날짜
	• rds-in-backup-plan • rds-instance-deletion-protection-enabled • rds-instance-iam-authentication-enabled • rds-logging-enabled • redshift-backup-enabled • waf-classic-logging-enabled • wafv2-logging-enabled 자세한 내용은 AWS Config 관리형 규칙 목록 단원을 참조하십시오.	
다중 계정 다중 리전 데이터 집계 영역 지원	이번 릴리스는 이제 아시아 태평양(홍콩) 및 중동(바레인) 리전에서 다중 계정 다중 리전 데이터 집계를 지원합니다. 자세한 내용은 Multi-Account Multi-Region Data Aggregation 및 에 대한 다중 계정 다중 리전 데이터 집계 문제 해결 AWS Config 섹션을 참조하세요.	2020년 7월 1일
고급 쿼리 리전 지원	이번 릴리스는 이제 아시아 태평양(홍콩) 및 중동(바레인) 리전에서 고급 쿼리를 지원합니다. 자세한 내용은 를 사용하여 리소스의 AWS 현재 구성 상태 쿼리 AWS Config 섹션을 참조하세요.	2020년 7월 1일

변경 사항	설명	릴리스 날짜
설명서 업데이트	설명서에서 다음 규칙에 대한 내용이 업데이트되었습니다. • ec2-managedinstance-association-compliance-status-check • iam-policy-no-statements-with-admin-access • required-tags • restricted-common-ports • rds-snapshots-public-prohibited • s3-bucket-policy-grantee-check	2020년 6월 30일
설명서 업데이트	설명서가 보안에 대한 정보로 업데이트되었습니다 AWS Config. 의 보안 AWS Config을(를) 참조하세요.	2020년 6월 24일
설명서 업데이트	AWS Control Tower Detective Guardrails 적합성 팩 템플릿이 업데이트되었습니다. 자세한 내용은 AWS Control Tower Detective Guardrails 적합성 팩 단원을 참조하십시오.	2020년 6월 4일
AWS Config 는 새 적합성 팩을 지원합니다.	이번 릴리스에서는가 NIST CSF 적합성 팩의 운영 모범 사례를 AWS Config 지원합니다. 자세한 내용은 NIST CSF 운영 모범 사례 단원을 참조하십시오.	2020년 5월 29일

변경 사항	설명	릴리스 날짜
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • dynamodb-pitr-enabled • dynamodb-table-encrypted-kms • ec2-ebs-encryption-by-default • rds-snapshot-encrypted • redshift-require-tls-ssl • s3-bucket-default-lock-enabled • s3-default-encryption-kms • securityhub-enabled • sns-encrypted-kms 자세한 내용은 AWS Config 관리형 규칙 목록 단원을 참조하십시오.	2020년 5월 28일

변경 사항	설명	릴리스 날짜
위임 관리자 지원	이번 릴리스에서는 관리 계정 외에도 조직의 위임된 멤버 계정에서 AWS Config 규칙 및 적합성 팩을 배포할 수 있습니다. API에 대한 자세한 내용은 AWS Config API 참조를 참조하세요. • PutOrganizationConfigRule • PutOrganizationConformancePack • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule • DeleteOrganizationConformancePack • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus 자세한 내용은 에 대한 서비스 제한 AWS Config 섹션을 참조하세요.	2020년 5월 27일

변경 사항	설명	릴리스 날짜
AWS Config 규칙 리전 지원	이번 릴리스에서는 아프리카(케이프타운) 및 유럽(밀라노) 리전에서 지원되는 AWS Config 규칙이 거의 없습니다. 규칙 및 규칙이 지원되는 리전의 세부 목록은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2020년 4월 28일
AWS Config 는 새 적합성 팩을 지원합니다.	이번 릴리스에서는가 두 개의 적합성 팩을 AWS Config 지원합니다. • AWS Control Tower Detective Guardrails 적합성 팩 • CIS 운영 모범 사례 자세한 내용은 에 대한 적합성 팩 샘플 템플릿 AWS Config 섹션을 참조하세요.	2020년 4월 22일
AWS Config 는 AWS Secrets Manager를 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 Secrets Manager 보안 암호에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2020년 4월 20일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • secretsmanager-rotation-enabled-check • secretsmanager-scheduled-rotation-success-check 자세한 내용은 AWS Config 관리형 규칙 목록 단원을 참조하십시오.	2020년 4월 16일

변경 사항	설명	릴리스 날짜
적합성 팩 리전 지원	이번 릴리스는 이제 아시아 태평양(홍콩) 및 중동(바레인)에서 적합성 팩을 지원합니다. 자세한 내용은 Conformance Packs 섹션을 참조하세요.	2020년 4월 8일
설명서 업데이트	AWS Config 제한은이 개발자 안내서에서 확인할 수 있습니다. 자세한 내용은 에 대한 서비스 제한 AWS Config 단원을 참조하십시오.	2020년 4월 8일
설명서 업데이트	AWS CloudFormation 레지스트리를 통해 관리되는 타사 리소스(즉, created/updated/deleted는에서 구성 항목 AWS Config 으로 자동으로 추적됩니다. 자세한 내용은 를 사용하여 타사 리소스 AWS Config 용를 사용하여 구성 기록 AWS CLI 단원을 참조하십시오.	2020년 3월 30일
설명서 업데이트	AWS Config 관리형 규칙은 정보를 포함하도록 AWS 리전 업데이트됩니다. 자세한 내용은 AWS Config 관리형 규칙 목록 단원을 참조하십시오.	2020년 3월 27일
AWS Config 에서 Amazon SNS 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 Amazon SNS 주제에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2020년 3월 6일
다중 계정 다중 리전 데이터 집계 영역 지원	이 릴리스는 유럽(스톡홀름) 리전에서 다중 계정 다중 리전 데이터 집계를 지원합니다. 자세한 내용은 Multi-Account Multi-Region Data Aggregation 섹션을 참조하세요.	2020년 3월 5일

변경 사항	설명	릴리스 날짜
고급 쿼리 리전 지원	이 릴리스는 유럽(스톡홀름) 리전에서 고급 쿼리를 지원합니다. 자세한 내용은 를 사용하여 리소스의 AWS 현재 구성 상태 쿼리 AWS Config 섹션을 참조하세요.	2020년 3월 5일
AWS Config 를 사용하면 구성 집계자를 사용하여 고급 쿼리를 실행할 수 있습니다.	이번 릴리스에서는 구성 집계기를 사용하여 리소스 구성 속성을 기반으로 고급 쿼리를 실행할 수 있는 지원을 AWS Config 추가하여 여러 계정 및 리전에서 동일한 쿼리를 실행할 수 있습니다. 자세한 내용은 를 사용하여 리소스의 AWS 현재 구성 상태 쿼리 AWS Config 단원을 참조하십시오. 이번 릴리스에서는 `SelectAggregateResourceConfig` API 를 AWS Config 추가합니다. 자세한 내용은 AWS Config API 참조의 SelectAggregateResourceConfig를 참조하세요.	2020년 2월 28일
AWS Config 에서 Amazon SQS 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 Amazon SQS 대기열에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2020년 2월 13일

변경 사항	설명	릴리스 날짜
AWS CloudFormation 적합성 팩 지원	이번 릴리스에서는 `AWS::Config::ConformancePack` 및 리소스에 대한 AWS CloudFormation 지원이 추가되었습니다`OrganizationConformancePack`. • AWS::Config::ConformancePack `AWS::Config::ConformancePack` 리소스를 사용하여 계정 및 리전과 AWS 조직 전체에 쉽게 배포할 수 있는 규칙 모음 AWS Config 인 적합성 팩을 생성합니다. • AWS::Config::OrganizationConformancePack `AWS::Config::OrganizationConformancePack` 리소스를 사용하여에 대한 정보가 있는 Organization Conformance Pack을 생성합니다. 가 멤버 계정에 AWS Config 생성하는 적합성 팩입니다.	2020년 2월 13일

변경 사항	설명	릴리스 날짜
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • api-gw-execution-logging-enabled • ec2-stopped-instance • elasticache-redis-cluster-automatic-backup-check • emr-master-no-public-ip • guardduty-non-archived-findings • rds-enhanced-monitoring-enabled • s3-account-level-public-access-blocks • sagemaker-endpoint-configuration-kms-key-configured • service-vpc-endpoint-enabled 자세한 내용은 AWS Config 관리형 규칙 목록 단원을 참조하십시오.	2019년 12월 20일

변경 사항	설명	릴리스 날짜
사용자 지정 리소스 유형에 대한 구성 기록	이 릴리스에서는 사용자 지정 리소스 유형에 대한 구성을 기록하는 지원을 AWS Config 소개합니다. 콘솔 AWS Config 및 API를 사용하여 AWS Config 타사 리소스의 구성 데이터를 에 게시하고 리소스 인벤토리 및 구성 기록을 보고 모니터링할 수 있습니다. APIs 자세한 내용은 를 사용하여 타사 리소스 AWS Config 용를 사용하여 구성 기록 AWS CLI 단원을 참조하십시오. API에 대한 자세한 내용은 AWS Config API 참조를 참조하세요. • DeleteResourceConfig • PutResourceConfig	2019년 11월 20일

변경 사항	설명	릴리스 날짜
적합성 팩	이번 릴리스에서는 적합성 팩을 AWS Config 소개합니다. 적합성 팩을 사용하면 AWS Config 규칙 및 수정 작업 모음을 패키징한 다음 전체 AWS 조직에 단일 엔터티로 함께 배포할 수 있습니다. 자세한 내용은 Conformance Packs 단원을 참조하십시오. API에 대한 자세한 내용은 AWS Config API 참조를 참조하세요. • DeleteOrganizationConformancePack • DeleteOrganizationConformancePack • DescribeConformancePacks • DescribeConformancePacks • DescribeConformancePackStatus • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetConformancePackComplianceDetails • GetConformancePackComplianceSummary • GetOrganizationConformancePackDetailedStatus, • PutConformancePack • PutOrganizationConformancePack	2019년 11월 19일

변경 사항	설명	릴리스 날짜
AWS Config 는 Amazon OpenSearch Service 및 AWS Key Management Service 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 Amazon OpenSearch Service 도메인 및 AWS Key Management Service 키에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2019년 11월 11일
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • dms-replication-not-public • emr-kerberos-enabled • internet-gateway-authorized-vpc-only • kms-cmk-not-scheduled-for-deletion • sagemaker-notebook-no-direct-internet-access • sagemaker-notebook-instance-kms-key-configured • shield-drt-access 자세한 내용은 AWS Config 관리형 규칙 목록 단원을 참조하십시오.	2019년 10월 10일

변경 사항	설명	릴리스 날짜
AWS Config 에서 Amazon RDS 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 Amazon Relational Database Service(RDS) DBCluster 및 DBClusterSnapshot에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2019년 9월 17일
AWS Config 에서 Amazon QLDB 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 Amazon Quantum Ledger Database(QLDB) 원장 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2019년 9월 10일
AWS Config 를 사용하면 AWS Config 규칙에서 평가한 규정 미준수 리소스에 자동 문제 해결을 적용할 수 있습니다.	이번 릴리스에서는 AWS Config 규칙에서 평가한 규정 미준수 리소스에 AWS Systems Manager 자동화 문서를 사용하여 자동 문제 해결을 적용하는 지원을 AWS Config 소개합니다. 자세한 내용은 를 사용하여 규정 미준수 리소스 문제 해결 AWS Config 단원을 참조하십시오. 이번 릴리스에서는 다음과 같은 새 APIs를 AWS Config 추가합니다. 자세한 내용은 AWS Config API 참조를 참조하세요. • PutRemediationExceptions • DescribeRemediationExceptions • DeleteRemediationExceptions	2019년 9월 5일

변경 사항	설명	릴리스 날짜
AWS Config 관리형 규칙 업데이트	이 릴리스에서는 다음 관리형 규칙을 AWS Config 지원합니다. • alb-http-to-https-redirection-check • api-gw-cache-enabled-and-encrypted • api-gw-endpoint-type-check • cloudtrail-s3-dataevents-enabled • cloudwatch-log-group-encrypted • ebs-snapshot-public-restorable-check • elb-deletion-protection-enabled • lambda-concurrency-check • lambda-dlq-check • lambda-inside-vpc • shield-advanced-enabled-autorenew • vpc-vpn-2-tunnels-up 자세한 내용은 AWS Config 관리형 규칙 목록 단원을 참조하십시오.	2019년 8월 22일

변경 사항	설명	릴리스 날짜
AWS Config 관리형 규칙 업데이트	이번 릴리스에서는가 다음 관리형 규칙을 AWS Config 업데이트합니다. • cloudfront-viewer-policy-https • ec2-instance-no-public-ip • ec2-security-group-attached-to-eni • efs-encrypted-check • elasticsearch-encrypted-at-rest • elasticsearch-in-vpc-only • redshift-cluster-public-access-check • vpc-sg-open-only-to-authorized-ports 자세한 내용은 AWS Config 관리형 규칙 목록 단원을 참조하십시오.	2019년 7월 31일
AWS Config 는 Amazon EC2 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 VPCEndpoint, VPCEndpointService VPCEndpointService 및 VPCPeeringConnection과 같은 Amazon EC2 리소스에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2019년 7월 12일

변경 사항	설명	릴리스 날짜
AWS Config 를 사용하면 조직 AWS 계정 내 모든에서 AWS Config 규칙을 관리할 수 있습니다.	이번 릴리스에서는 조직 AWS 계정 내 모든에서 규칙 관리에 AWS Config 대한 지원을 AWS Config 소개합니다. 조직의 모든 계정에서 AWS Config 규칙을 중앙에서 생성, 업데이트 및 삭제할 수 있습니다. 자세한 내용은 조직의 모든 계정에서 AWS Config 규칙 관리 단원을 참조하십시오. API에 대한 자세한 내용은 AWS Config API 참조를 참조하세요. • PutOrganizationConfigRule • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule	2019년 7월 9일
AWS Config 는 Amazon S3 및 Amazon EC2 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 Amazon S3 AccountPublicAccessBlock 리소스와 NatGateway, EgressOnlyInternetGateway 및 FlowLog와 같은 Amazon EC2 리소스에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2019년 5월 17일

변경 사항	설명	릴리스 날짜
AWS Config 관리형 규칙 업데이트	이번 릴리스에서는 다음과 같은 관리형 규칙을 AWS Config 업데이트합니다. • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited 자세한 내용은 AWS Config 관리형 규칙 목록 단원을 참조하십시오.	2019년 5월 7일
AWS Config 를 사용하면를 사용하여 문제 해결 작업을 삭제할 수 있습니다 AWS Management Console.	이 릴리스에서는를 사용하여 문제 해결 작업을 삭제할 수 있는 지원을 AWS Config 소개합니다 AWS Management Console. 자세한 내용은 를 사용하여 규정 미준수 리소스 문제 해결 AWS Config 단원을 참조하십시오.	2019년 4월 24일
AWS Config 는 새로운 관리형 규칙을 지원합니다.	이번 릴리스에서는 새로운 관리형 규칙인 fms-shield-resource-policy-check를 지원합니다. 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2019년 4월 7일

변경 사항	설명	릴리스 날짜
AWS Config 에서 Amazon API Gateway 리소스 유형 지원	이 릴리스에서는 AWS Config 를 사용하여 Api(WebSocket API), RestApi(REST API), 단계(WebSocket API 단계) 및 단계(REST API 단계)와 같은 Amazon API Gateway 리소스에 대한 구성 변경을 기록할 수 있습니다. RestApi WebSocket 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2019년 3월 20일
AWS Config 를 사용하면 고급 쿼리를 실행할 수 있습니다.	이 릴리스에서는 리소스 구성 속성을 기반으로 고급 쿼리를 실행할 수 있는 지원을 AWS Config 추가합니다. 자세한 내용은 를 사용하여 리소스의 AWS 현재 구성 상태 쿼리 AWS Config 단원을 참조하십시오. 이번 릴리스에서는 `SelectResourceConfig` API를 AWS Config 추가합니다. 자세한 내용은 AWS Config API 참조의 SelectResourceConfig를 참조하세요.	2019년 3월 19일

변경 사항	설명	릴리스 날짜
AWS Config 를 사용하면 AWS Config 리소스에 태그를 할당할 수 있습니다.	이번 릴리스에서는 및의 세 가지 AWS Config 리소스`ConfigRule`, `ConfigurationAggregator`, 에 대한 태그 기반 액세스 제어 지원을 AWS Config 소개합니다`AggregationAuthorization` . 자세한 내용은 AWS Config 리소스 태그 지정 단원을 참조하십시오. 이번 릴리스에서는 다음 데이터 형식을 사용하여 AWS Config 리소스의 태그를 추가, 제거 또는 나열할 수 있습니다. 자세한 내용은 AWS Config API 참조를 참조하세요. • ListTagsForResource • TagResource • UntagResource	2019년 3월 14일

변경 사항	설명	릴리스 날짜
AWS Config 를 사용하면 AWS Config 규칙에서 평가한 규정 미준수 리소스에 문제 해결을 적용할 수 있습니다.	이번 릴리스에서는 AWS Config 규칙에 따라 평가된 규정 미준수 리소스에 AWS Systems Manager 자동화 문서를 사용하여 문제 해결을 적용하는 지원을 AWS Config 소개합니다. 자세한 내용은 를 사용하여 규정 미준수 리소스 문제 해결 AWS Config 단원을 참조하십시오. 이번 릴리스에서는 다음과 같은 새 APIs를 AWS Config 추가합니다. 자세한 내용은 AWS Config API 참조를 참조하세요. • DeleteRemediationConfiguration • DescribeRemediationConfigurations • DescribeRemediationExecutionStatus • PutRemediationConfigurations • StartRemediationExecution	2019년 3월 12일

변경 사항	설명	릴리스 날짜
AWS Config 중국(닝샤) 리전에서 AWS Config 규칙 지원	이 릴리스는 중국(닝샤) 리전에서 54 AWS Config Rules만 지원합니다. 자세한 내용은 AWS Config 관리형 규칙 목록 단원을 참조하십시오. 그러나 AWS Config 는 현재 중국(닝샤) 리전에서 다음 규칙을 지원하지 않습니다. • acm-certificate-expiration-check • cmk-backing-key-rotation-enabled • cloudformation-stack-drift-detection-check • cloudformation-stack-notification-check • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check • dynamodb-table-encryption-enabled • elb-acm-certificate-required • encrypted-volumes • fms-webacl-resource-policy-check • fms-webacl-rulegroup-association-check	2019년 3월 12일

변경 사항	설명	릴리스 날짜
	• guardduty-enabled-centralized • lambda-function-public-access-prohibited • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-mfa-enabled • root-account-mfa-enabled • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-grantee-check • s3-bucket-policy-not-more-p ermissive • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited • s3-bucket-server-side-encryption-enabled • s3-bucket-ssl-requests-only	
AWS Config 는 새로운 관리형 규칙을 지원합니다.	이번 릴리스는 다음과 같은 새로운 관리형 규칙을 지원합니다. • iam-user-mfa-enabled • s3-bucket-policy-grantee-check 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2019년 1월 21일

변경 사항	설명	릴리스 날짜
AWS Config 는 Service Catalog 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 CloudFromation 제품, 프로비저닝된 제품 및 포트폴리오와 같은 Service Catalog 리소스에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2019년 1월 11일
서비스 연결 AWS Config 규칙 지원	이 릴리스에서는 계정에서 규칙을 생성하기 위해 다른 AWS 서비스를 지원하는 새 관리형 구성 AWS Config 규칙을 AWS Config 추가합니다. 자세한 내용은 서비스 연결 AWS Config 규칙 단원을 참조하십시오.	2018년 11월 20일
AWS Config 를 사용하면 리소스의 AWS 구성 데이터를 집계할 수 있습니다.	이 릴리스에서는 AWS 리소스의 구성 데이터를 집계하기 위한 지원을 AWS Config 소개합니다. 자세한 내용은 에 대한 집계자 대시보드에서 규정 준수 및 인벤토리 데이터 보기 AWS Config 단원을 참조하십시오. 이번 릴리스에서는 다음과 같은 새 APIs를 AWS Config 추가합니다. 자세한 내용은 AWS Config API 참조를 참조하세요. • BatchGetAggregateResourceConfig • GetAggregateDiscoveredResourceCounts • GetAggregateResourceConfig • ListAggregateDiscoveredResources	2018년 11월 19일

변경 사항	설명	릴리스 날짜
AWS Config 는 새로운 관리형 규칙을 지원합니다.	이번 릴리스는 다음과 같은 새로운 관리형 규칙을 지원합니다. • cloudformation-stack-drift-detection-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2018년 11월 19일

변경 사항	설명	릴리스 날짜
AWS Config 는 새로운 관리형 규칙을 지원합니다.	이번 릴리스는 다음과 같은 새로운 관리형 규칙을 지원합니다. • access-keys-rotated • cloud-trail-cloud-watch-logs-enabled • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • cmk-backing-key-rotation-enabled • iam-policy-no-statements-with-admin-access • iam-role-managed-policy-check • iam-root-access-key-check • iam-user-unused-credentials-check • mfa-enabled-for-iam-console-access • multi-region-cloudtrail-enabled • root-account-hardware-mfa-enabled • vpc-flow-logs-enabled 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2018년 11월 12일

변경 사항	설명	릴리스 날짜
AWS Config 는 새로운 관리형 규칙을 지원합니다.	이번 릴리스는 다음과 같은 새로운 관리형 규칙을 지원합니다. • dynamodb-table-encryption-enabled • elb-logging-enabled • rds-instance-public-access-check • vpc-default-security-group-closed 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2018년 10월 24일
규정 준수 기록 지원	이 릴리스에서는 AWS Config 이제가 AWS Config 규칙에서 평가한 리소스의 규정 준수 기록 저장을 지원합니다. 자세한 내용은 리소스 및 규칙 규정 준수 기록 타임라인 보기 단원을 참조하십시오.	2018년 10월 18일
다중 계정 다중 리전 데이터 집계 영역 지원	이 릴리스는 여섯 개의 새로운 리전에서 다중 계정 다중 리전 데이터 집계를 지원합니다. 자세한 내용은 Multi-Account Multi-Region Data Aggregation 섹션을 참조하세요.	2018년 10월 4일
AWS Config 는 AWS Config 규칙 APIs 작업에 대한 리소스 수준 권한을 지원합니다.	이 릴리스에서는가 특정 AWS Config 규칙 API 작업에 대한 리소스 수준 권한을 AWS Config 지원합니다. 지원되는 API에 대한 자세한 내용은 AWS Config 규칙 API 작업에 지원되는 리소스 수준 권한 섹션을 참조하세요.	2018년 10월 1일

변경 사항	설명	릴리스 날짜
AWS Config 에서 CodePipeline 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 AWS CodePipeline 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2018년 9월 12일
AWS Config 는 새로운 관리형 규칙을 지원합니다.	이번 릴리스는 다음과 같은 새로운 관리형 규칙을 지원합니다. • ec2-instance-managed-by-systems-manager • ec2-managedinstance-association-compliance-status-check • ec2-managedinstance-patch-compliance-status-check • guardduty-enabled-centralized • rds-snapshots-public-prohibited • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-not-more-permissive 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2018년 9월 5일
AWS Config 는 AWS Systems Manager 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 AWS Systems Manager 패치 규정 준수 및 연결 규정 준수 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2018년 8월 9일

변경 사항	설명	릴리스 날짜
AWS Config 를 사용하면를 사용하여 AWS Config 데이터를 삭제할 수 있습니다. AWS Management Console	이 릴리스에서는를 사용하여 보존 기간에 대한 지원을 AWS Config 소개합니다 AWS Management Console. 에서 `ConfigurationItems` 에 대한 사용자 지정 데이터 보존 기간을 AWS Management Console선택할 수 있습니다. 자세한 내용은 AWS Config 데이터 삭제 단원을 참조하십시오.	2018년 8월 7일
AWS Config 에서 AWS Shield 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 AWS Shield 보호 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2018년 8월 7일
AWS Config Support AWS PrivateLink	이번 릴리스에서는 AWS Config supports AWS PrivateLink를 통해 Amazon Virtual Private Cloud(VPC)와 AWS Config 전체 AWS 네트워크 내에서 데이터를 라우팅할 수 있습니다. 자세한 내용은 인터페이스 Amazon VPC 엔드포인트 AWS Config 와 함께 사용 단원을 참조하십시오.	2018년 7월 31일

변경 사항	설명	릴리스 날짜
AWS Config 를 사용하면 AWS Config 데이터를 삭제할 수 있습니다.	이 릴리스에서는 보존 기간에 대한 지원을 AWS Config 소개합니다.를 AWS Config 사용하면 `ConfigurationItems` 에 대한 보존 기간을 지정하여 데이터를 삭제할 수 있습니다. 자세한 내용은 AWS Config 데이터 삭제 단원을 참조하십시오. 이번 릴리스에서는 다음과 같은 새 APIs를 AWS Config 추가합니다. 자세한 내용은 AWS Config API 참조를 참조하세요. • PutRetentionConfiguration • DescribeRetentionConfigurations • DeleteRetentionConfiguration	2018년 5월 25일
AWS Config 는 새로운 관리형 규칙을 지원합니다.	이번 릴리스는 다음 두 가지 새로운 관리형 규칙을 지원합니다. • lambda-function-settings-check • s3-bucket-replication-enabled • iam-policy-blacklisted-check 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2018년 5월 10일
AWS Config 에서 AWS X-Ray 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 AWS X-Ray EncryptionConfig 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2018년 5월 1일

변경 사항	설명	릴리스 날짜
AWS Config 는 AWS Lambda 리소스 유형과 하나의 새 관리형 규칙을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 AWS Lambda 함수 리소스 유형에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오. 또한 이 릴리스는 lambda-function-public-access-prohibited 관리형 규칙을 지원합니다. 자세한 내용은 AWS Config 관리형 규칙 섹션을 참조하세요.	2018년 25월 4일
AWS Config 에서 AWS Elastic Beanstalk 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 AWS Elastic Beanstalk 애플리케이션, 애플리케이션 버전 및 환경 리소스에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2018년 24월 4일
AWS Config 는 새로운 관리형 규칙을 지원합니다.	이번 릴리스는 다음 두 가지 새로운 관리형 규칙을 지원합니다. • fms-webacl-resource-policy-check • fms-webacl-rulegroup-association-check 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2018년 4월 4일

변경 사항	설명	릴리스 날짜
다중 계정 다중 리전 데이터 집계	이번 릴리스에서는 다중 계정 다중 리전 데이터 집계를 AWS Config 소개합니다. 이 기능을 사용하면 여러 계정 또는 조직 및 여러 리전의 AWS Config 데이터를 집계자 계정으로 집계할 수 있습니다. 자세한 내용은 Multi-Account Multi-Region Data Aggregation 단원을 참조하십시오. 이번 릴리스에서는 다음과 같은 새 APIs를 AWS Config 추가합니다. 자세한 내용은 AWS Config API 참조를 참조하세요. • PutConfigurationAggregator • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregationAuthorization • DescribeAggregationAuthorizations • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfigRule • DescribeConfigurationAggregators • DescribeConfigurationAggregatorSourcesStatus • DeleteAggregationAuthorization • DeleteConfigurationAggregator	2018년 4월 4일

변경 사항	설명	릴리스 날짜
Amazon CloudWatch Events AWS Config 를 사용한 모니터링	이번 릴리스에서는 Amazon CloudWatch Events를 사용하여 AWS Config 이벤트 상태 변경을 감지하고 이에 대응합니다. 자세한 내용은 Amazon EventBridge AWS Config 를 사용한 모니터링 단원을 참조하십시오.	2018년 3월 29일
새로운 API 연산	이번 릴리스에서는 BatchGetResourceConfig API에 대한 지원을 AWS Config 추가하여 하나 이상의 리소스의 현재 상태를 일괄 검색할 수 있습니다.	2018년 3월 20일
AWS Config support AWS WAF RuleGroup 리소스 유형	이번 릴리스에서는 AWS Config 를 사용하여 AWS WAF RuleGroup 및 AWS WAF RuleGroup 리전 리소스에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2018년 2월 15일

변경 사항	설명	릴리스 날짜
AWS Config 는 새로운 관리형 규칙을 지원합니다.	이번 릴리스는 다음과 같은 새로운 관리형 규칙을 지원합니다. • elb-acm-certificate-required • elb-custom-security-policy-ssl-check • elb-predefined-security-policy-ssl-check • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • iam-group-has-users-check • s3-bucket-server-side-encryption-enabled 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2018년 1월 25일
AWS Config 는 Elastic Load Balancing 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 Elastic Load Balancing 클래식 로드 밸런서에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2017년 11월 17일

변경 사항	설명	릴리스 날짜
AWS Config 는 Amazon CloudFront 및 AWS WAF 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 CloudFront 배포 및 스트리밍 배포에 대한 구성 변경을 기록할 수 있습니다. 이번 릴리스에서는 AWS Config 를 사용하여 속도 기반 규칙, 규칙 및 웹 ACL과 같은 AWS WAF 및 AWS WAF 리전 리소스에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2017년 11월 15일
AWS Config 는 AWS CodeBuild 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 AWS CodeBuild 프로젝트에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2017년 10월 20일

변경 사항	설명	릴리스 날짜
AWS Config 는 Auto Scaling 리소스와 하나의 새로운 관리형 규칙을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 오토 Auto Scaling 리소스, 즉 그룹, 시작 구성, 예약된 작업 및 조정 정책에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오. 이 릴리스는 또한 다음과 같은 관리형 규칙을 지원합니다. • autoscaling-group-elb-healthcheck-required 자세한 내용은 AWS Config 관리형 규칙 섹션을 참조하세요.	2017년 9월 18일
AWS Config 는 AWS CodeBuild 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 AWS CodeBuild 프로젝트에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2017년 10월 20일

변경 사항	설명	릴리스 날짜
AWS Config 는 Auto Scaling 리소스와 하나의 새로운 관리형 규칙을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 오토 Auto Scaling 리소스, 즉 그룹, 시작 구성, 예약된 작업 및 조정 정책에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오. 이 릴리스는 또한 다음과 같은 관리형 규칙을 지원합니다. • autoscaling-group-elb-healthcheck-required 자세한 내용은 AWS Config 관리형 규칙 섹션을 참조하세요.	2017년 9월 18일
AWS Config 는 DynamoDB 테이블 리소스 유형과 하나의 새 관리형 규칙을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 DynamoDB 테이블에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오. 이 릴리스는 다음과 같은 관리형 규칙을 지원합니다. • dynamodb-autoscaling-enabled 자세한 내용은 AWS Config 관리형 규칙 섹션을 참조하세요.	2017년 9월 8일

변경 사항	설명	릴리스 날짜
AWS Config 는 Amazon S3에 대한 두 가지 새로운 관리형 규칙을 지원합니다.	이번 릴리스에서는 다음 두 가지 새로운 관리형 규칙을 지원합니다. • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited 자세한 내용은 AWS Config 관리형 규칙 섹션을 참조하세요.	2017년 8월 14일
AWS Config 콘솔의 새 페이지	AWS Config 콘솔에서 대시보드를 사용하여 다음을 확인할 수 있습니다. • 총 리소스 수 • 총 규칙 수 • 규칙 미준수 리소스 개수 • 미준수 규칙 수 자세한 내용은 AWS Config 대시보드 보기 섹션을 참조하세요.	2017년 7월 17일
새로운 API 연산	GetDiscoveredResourceCounts 작업을 사용하여 리소스 유형 수, 각 리소스 유형 수, 리전에서 기록 AWS Config 중인 총 리소스 수를 반환할 수 있습니다 AWS 계정.	2017년 7월 17일

변경 사항	설명	릴리스 날짜
AWS Config 는 AWS CloudFormation 스택 리소스 유형과 하나의 새 관리형 규칙을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 AWS CloudFormation 스택에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오. 이 릴리스는 다음과 같은 관리형 규칙을 지원합니다. • cloudformation-stack-notification-check 자세한 내용은 AWS Config 관리형 규칙 섹션을 참조하세요.	2017년 6월 7일
신규 및 업데이트된 콘텐츠	이 릴리스는 캐나다(중부) 리전 및 남아메리카(상파울루) 리전의 AWS Config 규칙에 대한 지원을 추가합니다. AWS Config 및 Config 규칙을 지원하는 모든 리전은의 AWS 리전 및 엔드포인트를 참조하세요AWS 일반 참조.	2017년 7월 5일
신규 및 업데이트된 콘텐츠	AWS Config 규칙은 AWS GovCloud (US) 리전에서 사용할 수 있습니다. 자세한 내용은 AWS GovCloud (US) 사용 설명서를 참조하십시오. 를 지원하는 리전은의 AWS 리전 및 엔드포인트를 AWS Config참조하세요AWS 일반 참조.	2017년 6월 8일

변경 사항	설명	릴리스 날짜
AWS Config 는 Amazon CloudWatch 경보 리소스 유형과 세 가지 새로운 관리형 규칙을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 Amazon CloudWatch 경보에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오. 이번 릴리스에서는 다음 세 가지 새로운 관리형 규칙을 지원합니다. • cloudwatch-alarm-action-check • cloudwatch-alarm-resource-check • cloudwatch-alarm-settings-check 자세한 내용은 AWS Config 관리형 규칙 섹션을 참조하세요.	2017년 6월 1일
신규 및 업데이트된 콘텐츠	이번 릴리스에서는 다음 관리형 규칙에 대한 애플리케이션 버전 번호 지정을 지원합니다. • ec2-managedinstance-applications-blacklisted • ec2-managedinstance-applications-required 자세한 내용은 AWS Config 관리형 규칙 섹션을 참조하세요.	2017년 6월 1일
신규 및 업데이트된 콘텐츠	이 릴리스는 아시아 태평양(뭄바이) 리전의 AWS Config 규칙에 대한 지원을 추가합니다. 자세한 내용은 AWS 일반 참조의 AWS 리전 및 엔드포인트를 참조하세요.	2017년 4월 27일

변경 사항	설명	릴리스 날짜
신규 및 업데이트된 콘텐츠	이번 릴리스에서는 처음으로 계정에 AWS Config 관리형 규칙을 추가할 수 있도록 업데이트된 콘솔 환경을 지원합니다. AWS Config 규칙을 처음 설정하거나 새 리전에서 설정할 때 이름, 설명 또는 레이블별로 AWS 관리형 규칙을 검색할 수 있습니다. 모두 선택을 선택하여 모든 규칙을 선택하거나 모두 지우기를 선택하여 모든 규칙을 지울 수 있습니다. 자세한 내용은 규칙 추가, 보기, 업데이트 및 삭제(콘솔)를 참조하세요.	2017년 4월 5일
AWS Config 는 새로운 관리형 규칙을 지원합니다.	이번 릴리스는 다음과 같은 새로운 관리형 규칙을 지원합니다. • acm-certificate-expiration-check • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-inventory-blacklisted • ec2-volume-inuse-check • iam-user-group-membership-check • iam-user-no-policies-check • s3-bucket-ssl-requests-only 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2017년 2월 21일

변경 사항	설명	릴리스 날짜
신규 및 업데이트된 콘텐츠	이 릴리스는 유럽(런던) 리전의 AWS Config 규칙에 대한 지원을 추가합니다. 자세한 내용은 AWS 일반 참조의 AWS 리전 및 엔드포인트를 참조하세요.	2017년 2월 21일
신규 및 업데이트된 콘텐츠	이 릴리스에서는 AWS Config 관리형 규칙에 대한 AWS CloudFormation 템플릿을 추가합니다. 템플릿을 사용하여 계정에 대한 관리형 규칙을 만들 수 있습니다. 자세한 내용은 AWS CloudFormation 템플릿을 사용하여 AWS Config 관리형 규칙 생성 섹션을 참조하세요.	2017년 2월 16일
신규 및 업데이트된 콘텐츠	이번 릴리스에서는 `PutEvaluations` API용 새로운 테스트 모드를 추가로 지원합니다. 사용자 지정 규칙에서 `TestMode` 파라미터를 true로 설정하여 AWS Lambda 함수가 AWS Config로 평가 결과를 전달하는지 여부를 확인할 수 있습니다. 기존 평가는 업데이트되지 않으며, 평가 결과가 AWS Config로 전송되지 않습니다. 자세한 내용은 AWS Config API 참조의 PutEvaluations를 참조하세요.	2017년 2월 16일
신규 및 업데이트된 콘텐츠	이 릴리스는 아시아 태평양(서울) 및 미국 서부(캘리포니아 북부) 리전의 AWS Config 규칙에 대한 지원을 추가합니다. 자세한 내용은 AWS 일반 참조의 AWS 리전 및 엔드포인트를 참조하세요.	2016년 21월 12일

변경 사항	설명	릴리스 날짜
신규 및 업데이트된 콘텐츠	이 릴리스는 유럽(런던) 리전 AWS Config 에서에 대한 지원을 추가합니다. 자세한 내용은 AWS 일반 참조의 AWS 리전 및 엔드포인트를 참조하세요.	2016년 12월 13일
신규 및 업데이트된 콘텐츠	이 릴리스는 캐나다(중부) 리전 AWS Config 에서에 대한 지원을 추가합니다. 자세한 내용은 AWS 일반 참조의 AWS 리전 및 엔드포인트를 참조하세요.	2016년 12월 8일
AWS Config 는 Amazon Redshift 리소스 유형과 두 가지 새로운 관리형 규칙을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 Amazon Redshift 클러스터, 클러스터 파라미터 그룹, 클러스터 보안 그룹, 클러스터 스냅샷, 클러스터 서브넷 그룹 및 이벤트 구독에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오. 이번 릴리스에서는 다음 두 가지 새로운 관리형 규칙을 지원합니다. • redshift-cluster-configuration-check • redshift-cluster-maintenancesettings-check 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2016년 7월 12일

변경 사항	설명	릴리스 날짜
신규 및 업데이트된 콘텐츠	이번 릴리스에서는 다음 새로운 관리형 규칙을 추가로 지원합니다. • dynamodb-throughput-limit-check 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2016년 7월 12일
신규 및 업데이트된 콘텐츠	이번 릴리스에서는 한 계정에서 리전당 최대 50개의 규칙을 만들 수 있도록 추가로 지원합니다. 자세한 내용은 AWS 일반 참조의 AWS Config 한도를 참조하세요.	2016년 7월 12일
AWS Config 는 Amazon EC2 Systems Manager에 대한 관리형 인스턴스 인벤토리 리소스 유형과 세 가지 새로운 관리형 규칙을 지원합니다.	이 릴리스에서는 AWS Config 를 사용하여 관리형 인스턴스 인벤토리를 지원하는 관리형 인스턴스의 소프트웨어 구성 변경을 기록할 수 있습니다. 자세한 내용은 Recording Software Configuration for Managed Instances 단원을 참조하십시오. 이번 릴리스에서는 다음 세 가지 새로운 관리형 규칙을 지원합니다. • ec2-managedinstance-inventory-blacklisted • ec2-managedinstance-applications-required • ec2-managedinstance-platform-check 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2016년 1월 12일

변경 사항	설명	릴리스 날짜
신규 및 업데이트된 콘텐츠	AWS Config 는 중국(베이징) 리전에서 사용할 수 있습니다.	2016년 10월 24일
AWS Config 는 Amazon S3 버킷 리소스와 두 가지 새로운 관리형 규칙을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 Amazon S3 버킷에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오. 이번 릴리스에서는 다음 두 가지 새로운 관리형 규칙을 지원합니다. • s3-bucket-logging-enabled • s3-bucket-versioning-enabled 자세한 내용은 AWS Config 관리형 규칙 섹션을 참조하세요.	2016년 10월 18일
신규 및 업데이트된 콘텐츠	이 릴리스에는 미국 동부(오하이오) 리전의 AWS Config 및 AWS Config 규칙에 대한 지원이 추가되었습니다. 자세한 내용은 AWS 일반 참조의 AWS 리전 및 엔드포인트를 참조하세요.	2016년 10월 17일

변경 사항	설명	릴리스 날짜
신규 및 업데이트된 관리형 규칙	이번 업데이트에서는 다음 8가지 새로운 관리형 규칙을 추가로 지원합니다. • approved-amis-by-id • approved-amis-by-tag • db-instance-backup-enabled • desired-instance-type • ebs-optimized-instance • iam-password-policy • rds-multi-az-support • rds-storage-encrypted 다음 규칙에 대해 여러 파라미터 값을 지정할 수 있습니다. • desired-instance-tenancy • required-tags 자세한 내용은 AWS Config 관리형 규칙 목록 섹션을 참조하세요.	2016년 10월 4일
AWS Config 콘솔에 대한 신규 및 업데이트된 콘텐츠	이 업데이트는 AWS Config 타임라인에서 AWS CloudTrail API 활동을 볼 수 있는 지원을 추가합니다. CloudTrail이 계정에 대해 로깅하면 리소스의 구성 변경에 대한 생성, 업데이트 및 삭제 API 이벤트를 볼 수 있습니다. 자세한 내용은 를 사용하여 AWS 리소스에 대한 규정 준수 기록 보기 AWS Config 섹션을 참조하세요.	2016년 9월 06일

변경 사항	설명	릴리스 날짜
AWS Config 는 Elastic Load Balancing 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 Elastic Load Balancing 애플리케이션 로드 밸런서에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2016년 8월 31일
신규 및 업데이트된 콘텐츠	이 릴리스는 아시아 태평양(싱가포르) 및 아시아 태평양(시드니) 리전의 AWS Config 규칙에 대한 지원을 추가합니다. 자세한 내용은 AWS 일반 참조의 AWS 리전 및 엔드포인트를 참조하세요.	2016년 8월 18일
AWS Config 규칙에 대한 신규 및 업데이트된 콘텐츠	이번 업데이트에서는 구성 변경 및 사용자가 선택한 주기적 간격으로 모두 트리거할 수 있는 규칙을 만들 수 있도록 추가로 지원합니다. 자세한 내용은 AWS Config 규칙의 구성 요소 단원을 참조하십시오. 또한 이번 업데이트에서는 규칙을 기준으로 리소스를 수동으로 평가하고 평가 결과를 삭제할 수 있도록 추가로 지원합니다. 자세한 내용은 AWS Config 규칙을 사용하여 리소스 평가 섹션을 참조하세요. 또한 이번 업데이트에서는 사용자 지정 규칙을 사용하여 추가 리소스 유형을 평가할 수 있도록 추가로 지원합니다.	2016년 7월 25일

변경 사항	설명	릴리스 날짜
AWS Config 는 Amazon RDS 및 AWS Certificate Manager (ACM) 리소스 유형을 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 Amazon Relational Database Service(RDS) DB 인스턴스, DB 보안 그룹, DB 스냅샷, DB 서브넷 그룹 및 이벤트 구독에 대한 구성 변경을 기록할 수 있습니다. AWS Config 를 사용하여 ACM에서 제공하는 인증서에 대한 구성 변경을 기록할 수도 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2016년 7월 21일
구성 레코더 관리에 대한 업데이트된 정보	이번 업데이트에서는 구성 레코더 작업에 구성 레코더를 삭제하고 이름을 바꾸는 단계를 추가했습니다.	2016년 7월 07일
간소화된 역할 만들기 및 업데이트된 정책	이 업데이트를 통해에 대한 IAM 역할 생성 AWS Config 이 간소화됩니다. 이 개선 사항은 Config 규칙을 지원하는 리전에서 이용할 수 있습니다. 이 개선 사항을 지원하기 위해 콘솔 AWS Config 로 설정의 단계, AWS Config 전송 채널에 대한 Amazon S3 버킷에 대한 권한의 정책 예제, 에 대한 자격 증명 기반 정책 예제 AWS Config의 정책 예제가 업데이트되었습니다.	2016년 3월 31일
Config 규칙의 함수 및 이벤트 예제	이 업데이트는 업데이트된 예제 함수를 제공합니다.	2016년 3월 29일

변경 사항	설명	릴리스 날짜
AWS Config 규칙 GitHub 리포지토리	이 업데이트에서 AWS Config 규칙 GitHub 리포지토리에 대한 정보가 AWS Config 규칙을 사용하여 리소스 평가에 추가되었습니다. 이 리포지토리는 AWS Config 사용자가 개발하고 기여하는 사용자 지정 규칙에 대한 샘플 함수를 제공합니다.	2016년 3월 1일
AWS Config 규칙	이 릴리스에는 AWS Config 규칙이 도입되었습니다. 규칙을 사용하면 AWS Config 를 사용하여 AWS 리소스가 원하는 구성을 준수하는지 평가할 수 있습니다. 자세한 내용은 AWS Config 규칙을 사용하여 리소스 평가 단원을 참조하십시오.	2015년 12월 18일
AWS Config 에서 IAM 리소스 유형 지원	이번 릴리스에서는 AWS Config 를 사용하여 IAM 사용자, 그룹, 역할 및 고객 관리형 정책에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2015년 12월 10일
AWS Config 는 EC2 전용 호스트를 지원합니다.	이번 릴리스에서는 AWS Config 를 사용하여 EC2 전용 호스트에 대한 구성 변경을 기록할 수 있습니다. 자세한 내용은 에 대해 지원되는 리소스 유형 AWS Config 단원을 참조하십시오.	2015년 11월 23일

변경 사항	설명	릴리스 날짜
업데이트된 권한 정보	이 업데이트는 AWS Config다음 AWS 관리형 정책에 대한 정보를 추가합니다. • `AWS_ConfigRole` - AWS Config 에게 리소스에 대한 구성 세부 정보를 가져올 수 있는 권한을 부여합니다. 자세한 내용은 구성 세부 정보를 가져오기 위한 IAM 역할 정책 단원을 참조하십시오. • `AWSConfigUserAccess` - AWS Config 사용자에게 읽기 전용 액세스 권한을 부여합니다. 자세한 내용은 에 대한 읽기 전용 액세스 AWS Config 단원을 참조하십시오.	2015년 10월 19일
AWS Config 규칙 미리 보기	이 릴리스에서는 AWS Config 규칙 미리 보기를 소개합니다. 규칙을 사용하면 AWS Config 를 사용하여 AWS 리소스가 원하는 구성을 준수하는지 평가할 수 있습니다. 자세한 내용은 AWS Config 규칙을 사용하여 리소스 평가 단원을 참조하십시오.	2015년 10월 7일
신규 및 업데이트된 콘텐츠	이 릴리스에서는에서 검색 AWS Config 한 리소스를 조회할 수 있는 기능이 추가되었습니다. 자세한 내용은 에서 검색한 리소스 조회 AWS Config 단원을 참조하십시오.	2015년 8월 27일
신규 및 업데이트된 콘텐츠	이번 릴리스에서는 AWS Config 가 기록하는 리소스 유형을 선택할 수 있는 기능이 추가되었습니다. 자세한 내용은 를 사용하여 AWS 리소스 기록 AWS Config 섹션을 참조하세요.	2015년 6월 23일

변경 사항	설명	릴리스 날짜
신규 및 업데이트된 콘텐츠	이번 릴리스에서는 아시아 태평양(도쿄), 아시아 태평양(싱가포르), 유럽(프랑크푸르트), 남아메리카(상파울루) 및 미국 서부(캘리포니아 북부) 리전에 대한 지원을 추가했습니다. 자세한 내용은 AWS 리전 및 엔드포인트를 참조하세요.	2015년 4월 6일
새 안내서	이 릴리스는 AWS Config을 도입했습니다.	2014년 11월 12일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.