



AMS 고급 개념 및 절차

AMS 고급 사용 설명서



버전 October 3, 2025

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

AMS 고급 사용 설명서: AMS 고급 개념 및 절차

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

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon 계열사, 관련 업체 또는 Amazon의 지원 업체 여부에 상관없이 해당 소유자의 자산입니다.

Table of Contents

AWS Managed Services란 무엇입니까?	1
이 가이드 정보	2
운영 계획	2
운영 계획 가속화	2
고급 운영 계획	3
시작하기	3
주요 용어	3
서비스 설명	9
AWS Managed Services(AMS) AMS Advanced 운영 계획 기능	9
수행하는 작업, 수행하지 않는 작업	14
AMS 책임 매트릭스(RACI)	15
AMS 환경 기본 구성 요소	34
AMS 계정 제한	37
AMS 서비스 수준 목표(SLOs)	39
지원되는 AWS 서비스	40
지원되는 구성	43
지원되지 않는 운영 체제	45
AMS 고급 인터페이스	46
VPC 엔드포인트	47
AMS 보호 네임스페이스	48
AMS 예약 접두사	49
AMS 유지 관리 기간	50
AMS 정보 리소스	51
AMS 규정 준수	51
AMS 지원 규정 준수 표준	52
공동 책임	55
AMS Amazon Machine Image(AMIs)	55
보안 강화 AMIs	58
AD FS와 AMS 간의 통합 작동 방식	58
AMS 관리형 Active Directory	60
애플리케이션 배포	62
서비스 관리	64
계정 거버넌스	64
서비스 시작	64

고객 관계 관리(CRM)	65
CRM 프로세스	66
CRM 회의	66
CRM 회의 계약	67
CRM 월별 보고서	68
비용 최적화	69
비용 최적화 프레임워크	69
비용 최적화 책임 매트릭스	71
서비스 시간	73
도움말 가져오기	73
계획된 이벤트 관리	74
AMS PEM 기준	74
PEM 유형	74
AMS PEM 프로세스	75
PEM FAQs	75
네트워크 아키텍처	77
MALZ 네트워크 아키텍처	77
다중 계정 랜딩 존 네트워크 아키텍처 정보	77
단일 MALZ 또는 여러 MALZs 선택	79
다중 계정 랜딩 존 계정	84
SALZ 네트워크 아키텍처	114
AMS 단일 계정 랜딩 존 공유 서비스	115
AMS 설정	116
AMS 기본 설정	117
DNS 확인 기본값(MALZ)	117
EC2 IAM 인스턴스 프로파일	118
AMS의 기준 모니터링 알림	125
로그 보존 및 교체 기본값	139
AMS 콘솔 사용	140
AMS API 및 CLI 사용	142
REST 호출을 위한 AMS API HTTP 엔드포인트	142
AMS CLI 설치 또는 업그레이드	142
CLI, Ruby, Python 및 Java에서 AMS API 사용	144
AMS에서 자체 EPS 사용	153
계정에 대해 BYOEPS 활성화	154
AMS 알림 수신	157

SNS를 사용한 AMS AMI 알림	158
서비스 알림	162
RFC 상태 변경 알림	162
프라이빗 및 퍼블릭 DNS 설정	166
AMS 송신 트래픽 관리	167
IAM 리소스 배포	168
자동 IAM 프로비저닝	169
IAM 역할 및 프로파일을 사용하여 권한 설정	187
새 IAM 사용자 역할 또는 인스턴스 프로파일 요청	188
IAM 역할 정책 설명을 사용하여 권한 제한	188
Amazon EC2 IAM 인스턴스 프로파일로 권한 제한	190
AD FS 클레임 규칙 및 SAML 설정	190
ADFS 클레임 규칙 구성	190
웹 콘솔	191
SAML을 사용한 API 및 CLI 액세스	191
네트워크 ACL로 제한	195
Outposts의 AMS	196
AWS Outposts 설치 및 운영 관리	196
에서 AMS 관리형 리소스 프로비저닝 AWS Outposts	198
의 AMS 제한 사항 AWS Outposts	199
AWS Outposts 규정 준수에 대한 AMS	200
AMS AWS Outposts FAQs	200
태그 사용	202
AMS 인프라 자동 태그 지정	203
AMS 권장 태그	205
대량 업데이트 정보 태그 지정	209
리소스 스케줄러	210
Resource Scheduler 배포	211
Resource Scheduler 사용자 지정	211
Resource Scheduler 사용	212
AMS Resource Scheduler 비용 예측기	212
AMS Resource Scheduler 모범 사례	214
AWS Systems Manager AMS Advanced의	215
사용 가능한 AMS Advanced SSM 문서	216
AMS Advanced SSM 문서 버전	216
Systems Manager 요금	216

AMS 계정 오프보드	217
단일 계정 랜딩 존 계정에서 오프보드	217
다중 계정 랜딩 존 계정에서 오프보드	221
변경 관리 모드	238
모드 개요	239
AMS의 모드 및 계정 유형	239
AMS 모드 및 애플리케이션 또는 워크로드	242
AMS 모드의 실제 사용 사례	247
RFC 모드	250
RFCs 대해 알아보기	251
변경 유형이란 무엇입니까?	286
RFC 오류 문제 해결	297
직접 변경 모드	306
직접 변경 모드 시작하기	307
보안 및 규정 준수	309
직접 변경 모드에서 변경 관리	314
Direct Change 모드를 사용하여 스택 생성	316
직접 변경 모드 사용 사례	319
개발자 모드	320
개발자 모드 시작하기	321
보안 및 규정 준수	323
변경 관리	324
인프라 프로비저닝	329
탐지 제어	330
로깅, 모니터링 및 이벤트 관리	330
인시던트 관리	330
패치 관리	330
연속성 관리	331
보안 및 액세스 관리	331
AMS의 셀프 서비스 프로비저닝 모드	331
AMS에서 SSP 모드 시작하기	332
Amazon API Gateway	333
Alexa for Business	334
Amazon AppStream 2.0	335
Amazon Athena	337
Amazon Bedrock	338

Amazon CloudSearch	339
Amazon CloudWatch Synthetics	340
Amazon Cognito	341
Amazon Comprehend	343
Amazon Connect	344
Amazon Data Firehose	345
Amazon DevOps Guru	346
Amazon DocumentDB(MongoDB 호환)	347
Amazon DynamoDB	348
Amazon Elastic 컨테이너 레지스트리	349
EC2 Image Builder	350
의 Amazon ECS AWS Fargate	352
의 Amazon EKS AWS Fargate	354
Amazon EMR	357
Amazon EventBridge	360
Amazon Forecast	362
Amazon FSx	364
Amazon FSx for OpenZFS	366
Amazon FSx for NetApp ONTAP	367
Amazon Inspector Classic	368
Amazon Kendra	370
Amazon Kinesis Data Streams	370
Amazon Kinesis Video Streams	371
Amazon Lex	372
Amazon MQ	373
Amazon Managed Service for Apache Flink	374
Amazon Managed Streaming for Apache Kafka	375
– Amazon Managed Service for Prometheus	376
Amazon Personalize	377
Amazon QuickSight	379
Amazon Rekognition	381
Amazon SageMaker AI	382
Amazon Simple Email Service	385
Amazon Simple Workflow Service	386
Amazon Textract	387
Amazon Transcribe	387

Amazon WorkSpaces	388
AMS 코드 서비스	390
AWS Amplify	393
AWS AppSync	394
AWS App Mesh	395
AWS Audit Manager	396
AWS Batch	397
AWS Certificate Manager	398
AWS Private Certificate Authority	399
AWS CloudEndure	402
AWS CloudHSM	403
AWS CodeBuild	404
AWS CodeCommit	405
AWS CodeDeploy	407
AWS CodePipeline	408
AWS Compute Optimizer	409
AWS DataSync	411
AWS Device Farm	412
AWS Elastic Disaster Recovery	413
AWS Elemental MediaConvert	414
AWS Elemental MediaLive	415
AWS Elemental MediaPackage	416
AWS Elemental MediaStore	417
AWS Elemental MediaTailor	418
AWS Global Accelerator	418
AWS Glue	419
AWS Lake Formation	421
AWS Lambda	422
AWS License Manager	423
AWS Migration Hub	424
AWS Outposts	425
AWS Resilience Hub	425
AWS Secrets Manager	426
AWS Security Hub	429
AWS Service Catalog AppRegistry	430
AWS Shield	431

AWS Snowball Edge	432
AWS Step Functions	433
AWS Systems Manager 파라미터 스토어	434
AWS Systems Manager 자동화	435
AWS Transfer Family	438
AWS Transit Gateway	440
AWS WAF	441
AWS Well-Architected Tool	442
AWS X-Ray	442
VM Import	443
고객 관리형 모드	445
고객 관리형 모드 시작하기	445
AMS 및 AWS Service Catalog	445
Service Catalog 시작하기	446
시작하기 전에 AMS의 Service Catalog	446
필요한 데이터 찾기(SKMS)	450
서비스 지식 관리란 무엇입니까?	450
VPC IDs 찾기	451
서브넷 IDs 찾기	453
AMI IDs 찾기	455
보안 그룹(SG) IDs 찾기	457
IAM 엔터티 찾기	457
스택 IDs 찾기	458
인스턴스 IDs 또는 IP 주소 찾기	460
ARNs 찾기	462
ARN으로 리소스 찾기	464
계정 설정 찾기	465
FQDNs 찾기	466
가용 영역(AZs) 찾기	467
SNS 주제 찾기	467
백업 설정 찾기	468
액세스 관리	469
액세스 관리란 무엇입니까?	469
계정에 액세스하는 이유와 시기	470
루트를 사용하는 방법 및 시기	474
AMS Advanced 콘솔 및 Amazon EC2 액세스	475

AWS 관리 콘솔 및 AMS 콘솔 액세스	476
임시 AMS 콘솔 액세스	476
Bastion을 사용하여 인스턴스에 액세스	477
DNS 친화적인 접속 이름	478
단일 계정 랜딩 존(SALZ) 접속 비용 절감	480
접속 IP 주소 사용	480
인스턴스 액세스 예제	481
AMS 계정의 팀 또는 역할 기반 액세스 제어	491
자동화된 EC2 인스턴스 구성	492
자동 인스턴스 구성을 위한 사전 조건	492
SSM 에이전트 자동 설치	493
사전 조건	493
SSM 에이전트의 자동 설치 요청	494
SSM 에이전트 자동 설치 작동 방식	494
자동 변경 사항	494
Linux 인스턴스에서 코드 자동 업데이트	495
Linux 인스턴스에서 PBIS 자동 업데이트	495
SSM 및 CloudWatch 에이전트의 최소 버전 자동 업데이트	496
CloudWatch 구성 파일, 세부 정보 업데이트	497
자동으로 구성된 로그	498
모니터링 및 이벤트 관리	500
모니터링이란 무엇입니까?	501
AMS 모니터링 시스템은 무엇을 모니터링합니까?	502
Active Directory Trust의 단일 계정 랜딩 존 사전 모니터링	502
모니터링 작동 방식	503
EC2 인스턴스 그룹화된 알림	504
태그 기반 알림	505
계정에 대한 모니터링 구성 보기	506
계정의 모니터링 구성 변경	506
AMS의 애플리케이션 인식 인시던트 알림	507
AMS 계정에서 AppRegistry 프로비저닝 및 애플리케이션 생성	507
태그를 생성하여 사례 보강 활성화	507
애플리케이션에 대한 AMS 지원 사례 심각도 사용자 지정	508
필요한 권한 검토	509
OpsCenter 사용	509
경고 알림	510

알림 수신	510
태그 기반 알림	510
알림의 AMS 자동 문제 해결	511
추가 CloudWatch 경보 생성	518
사용자 지정 CloudWatch 지표 및 경보 생성	520
.Net 및 SQL Server용 CloudWatch Application Insights 사용	521
AMS 이벤트 라우터	522
AMS에서 배포한 Amazon EventBridge 관리형 규칙	522
AMS에 대한 관리형 규칙 생성	522
AMS에 대한 관리형 규칙 편집	523
AMS에 대한 관리형 규칙 삭제	523
신뢰할 수 있는 수정자	523
주요 이점	523
신뢰할 수 있는 수정자 작동 방식	524
주요 용어	524
신뢰할 수 있는 문제 해결사 시작하기	525
지원되는 Compute Optimizer 권장 사항	528
지원되는 Trusted Advisor 검사	532
검사 문제 해결 구성	579
실행 모드 결정 워크플로	583
문제 해결 자습서 구성	583
문제 해결 작업	585
문제 해결 로그	589
모범 사례	592
FAQ	592
로그 관리	595
로그 관리란 무엇입니까?	595
AMS 로깅 작동 방식	595
로그 액세스	596
AMS 집계 서비스 로그	596
AMS 공유 서비스 로그	609
Amazon Elastic Compute Cloud(Amazon EC2) - 시스템 수준 로그	611
Splunk와 통합	613
로그 구성 사용자 지정	613
CloudWatch 로그 보존 변경	613
지원되는 서비스에 대한 로깅 활성화	613

보안 관리	615
AMS의 데이터 보호	615
Amazon Macie	616
GuardDuty	617
Amazon Route 53 Resolver DNS 방화벽	619
AWS Certificate Manager (ACM) 인증서	621
AMS의 데이터 암호화	621
자격 증명 및 액세스 관리	623
다중 계정 랜딩 존(MALZ) IAM 보호	623
ID를 통한 인증	623
보안 이벤트 로깅 및 모니터링	644
엔드포인트 보안(EPS)	644
맬웨어 완화 프로세스	649
Amazon Inspector 보안	650
AMS 인시던트 대응	652
규정 준수 확인	652
의 규정 준수 상태를 보는 다중 계정 랜딩 존 AWS Config 규칙	653
AMS 다중 계정 랜딩 존 서비스 제어 정책 제한	654
복원성	654
인프라 보안	654
보안 모범 사례	686
AMS 다중 계정 랜딩 존 EPS 기본값이 아닌 설정	686
AMS 가드레일	686
MALZ 서비스 제어 정책	686
보안 인시던트 대응	686
작동 방법	687
준비	687
감지	688
분석	689
격리	690
근절	692
복구	692
사후 인시던트 보고서	692
보안 인시던트 대응 런북	693
AMS Advanced의 변경 요청 보안 검토	698
고객 보안 위험 관리 프로세스	699

AMS Advanced 기술 표준	699
AMS Advanced의 표준 제어	700
환경에서 보안 위험이 높거나 매우 높은 변경 사항	722
연속성 관리	725
연속성 관리란 무엇입니까?	725
연속성 관리 작동 방식	725
백업 계획	725
백업 저장소	729
백업 변경 유형	730
백업 모니터링 및 보고	731
재해 복구 응답	731
재해 복구 계획	732
다중 사이트 또는 고가용성(HA)	732
웜 대기	733
파일럿 라이트	734
백업 및 복원	735
패치 관리	740
AMS 패치 오케스트레이터: 태그 기반 패치 적용 모델	741
패치 오케스트레이터 사용	742
패치 오케스트레이터 사전 조건	745
패치 창	746
패치 알림	747
패치 기준	750
패치 오케스트레이터 예약 태그	750
온디맨드 패치 적용	751
AMS 표준 패치 적용	751
지원되는 운영 체제	752
지원되는 패치	753
패치 및 인프라 설계	755
AMS 표준 패치 적용 방식	756
AMS 표준 패치 적용 실패	760
AMS 표준 패치에서 수행할 수 있는 작업	760
AMS 표준 패치 FAQs	764
서비스 커밋 패치 적용	766
표준 패치 적용	766
중요 패치 적용	767

보고서 및 옵션	771
요청 시 보고서	771
AMS 패치 보고서	772
AMS 백업 보고서	779
인시던트 방지 및 상위 화자 보고서 모니터링	782
결제 요금 세부 정보 보고서	784
신뢰할 수 있는 수정자 보고서	785
셀프 서비스 보고서	788
내부 API 작업	789
패치 보고서(일별)	792
백업 보고서(일별)	801
인시던트 보고서(주별)	805
결제 보고서(월별)	807
집계된 보고서	810
AMS 셀프 서비스 보고서 대시보드	812
데이터 보존 정책	818
SSR에서 오프보드	818
지원 받기	819
인시던트 관리	819
인시던트 관리란 무엇입니까?	820
인시던트 관리 서비스 약정	821
인시던트 관리 예제	824
서비스 요청 관리	829
서비스 요청을 사용해야 하는 경우	830
서비스 요청 관리 작동 방식	831
서비스 요청 테스트	832
서비스 요청 생성	832
서비스 요청 모니터링 및 업데이트	834
AMS 생성 서비스 요청에 응답	836
결제 질문	836
온디맨드 작업	837
온디맨드 AMS 작업 요청	843
Operations on Demand 오퍼링 변경	843
문서 기록	845
이전 업데이트	860
.....	dccclxxxvi

AWS Managed Services란 무엇입니까?

Amazon Web Services()의 인프라 운영 관리인 AWS Managed Services(AMS)에 오신 것을 환영합니다. AMS는 AWS 인프라를 지속적으로 관리하는 엔터프라이즈 서비스입니다.

이 사용 설명서는 IT 및 애플리케이션 개발자 전문가를 대상으로 합니다. IT 기능, 네트워킹 및 애플리케이션 배포 용어와 사례에 대한 기본적인 이해를 가정합니다.

AMS는 모범 사례를 구현하고 인프라를 유지 관리하여 운영 오버헤드와 위험을 줄입니다. AMS는 인프라를 프로비저닝, 실행 및 지원하는 전체 수명 주기 서비스를 제공하고 변경 요청, 모니터링, 패치 관리, 보안 및 백업 서비스와 같은 일반적인 활동을 자동화합니다. AMS는 기업 및 보안 인프라 정책을 적용하고 선호하는 개발 접근 방식을 사용하여 솔루션과 애플리케이션을 개발할 수 있습니다.

AMS 아키텍처를 더 잘 이해하려면 [다음 다이어그램을 참조하세요](#).

주제

- [이 AMS 사용 설명서 정보](#)
- [AMS 운영 계획](#)
- [AWS Managed Services 시작하기](#)
- [AMS 키 용어](#)
- [서비스 설명](#)
- [AMS 정보 리소스](#)
- [AMS 규정 준수](#)
- [AMS Amazon Machine Image\(AMIs\)](#)
- [AD FS와 AMS 간의 통합 작동 방식](#)
- [AMS 관리형 Active Directory](#)
- [AMS 애플리케이션 배포](#)

Note

새 AWS 리전 가 자주 추가됩니다. 최신 AMS 지원 운영 체제 AWS 리전와 최신 AMS 지원 운영 체제는 섹션을 참조하세요 [지원되는 구성](#).

에 대한 자세한 내용은 [관리를 AWS 리전](#) AWS 리전참조하세요.

AMS는 사용자의 피드백을 기반으로 서비스를 지속적으로 개선하고자 합니다. 여러 메커니즘을 사용하여 셀프 서비스를 활성화하고, 반복 작업을 자동화하고, 릴리스될 때 새로운 AWS 서비스 및 기능을 구현합니다. 언제든지 AMS 서비스 요청을 제출하여 새로운 기능 또는 기능 개선 사항을 제안할 수 있습니다.

AMS 업무 시간은 하루 24시간, 주 7일, 1년 365일입니다.

AMS는 IT 서비스를 비즈니스 요구 사항에 맞추는 데 중점을 둔 IT 서비스 관리(ITSM)에 대한 일련의 관행을 따릅니다.

이 AMS 사용 설명서 정보

이 사용 설명서는 다중 계정 또는 단일 계정 랜딩 존이 있는 AMS Advanced 고객을 대상으로 합니다. AMS 랜딩 존 상품에 대한 자세한 내용은 [AMS 키 용어](#)를 참조하세요. [또한 다중 계정 랜딩 존 아키텍처](#) 및 [단일 계정 랜딩 존 아키텍처](#)를 참조하세요.

AMS 운영 계획

AWS Managed Services(AMS)는 AMS Accelerate와 AMS Advanced라는 두 가지 운영 플랜과 함께 사용할 수 있습니다. 운영 계획은 특정 기능 세트를 제공하며 서비스, 기술 기능, 요구 사항, 가격 및 제한 수준이 다릅니다. 운영 계획을 통해 각 AWS 워크로드에 적합한 규모의 운영 기능을 유연하게 선택할 수 있습니다. 이 섹션에서는 계정에 가장 적합한 운영 계획을 이해할 수 있도록 기능 및 차이점과 각 계획과 관련된 책임, 기능 및 이점을 간략하게 설명합니다.

두 운영 계획에 대한 자세한 기능 비교는 [AWS Managed Services 기능](#)을 참조하세요.

AMS Accelerate 운영 계획

AMS Accelerate는 신규 또는 기존 AWS 환경의 day-to-day 인프라 관리를 운영하는 데 도움이 되는 AMS 운영 계획입니다. AMS Accelerate는 모니터링, 인시던트 관리 및 보안과 같은 운영 서비스를 제공합니다. 또한 AMS Accelerate는 정기적인 패치가 필요한 Amazon EC2 기반 워크로드에 대한 선택적 패치 추가 기능을 제공합니다.

AMS Accelerate를 사용하면 AMS Accelerate를 운영 AWS 계정 할 리전, AMS Accelerate를 운영할 AWS 리전, 필요한 추가 기능, 필요한 서비스 수준 계약(SLAs)을 결정할 수 있습니다. 자세한 내용은 [AMS Accelerate 운영 계획 사용](#) 및 [서비스 설명](#)을 참조하세요.

AMS Advanced 운영 계획

AMS Advanced는 인프라를 프로비저닝, 실행 및 지원하기 위한 전체 수명 주기 서비스를 제공합니다. AMS Accelerate에서 제공하는 운영 서비스 외에도 AMS Advanced에는 랜딩 존 관리, 인프라 변경 및 프로비저닝, 액세스 관리, 엔드포인트 보안과 같은 추가 서비스도 포함되어 있습니다.

AMS Advanced는 AWS 워크로드를 마이그레이션하고 AMS 운영 서비스를 받는 랜딩 존을 배포합니다. 관리형 다중 계정 랜딩 존은 인증, 보안, 네트워킹 및 로깅을 용이하게 하기 위해 인프라로 사전 구성되어 있습니다.

또한 AMS Advanced에는 무단 액세스 또는 AWS 인프라에 대한 위험한 변경 구현을 방지하여 워크로드를 보호하는 변경 및 액세스 관리 시스템이 포함되어 있습니다. 고객은 AMS Advanced 계정에서 대부분의 변경 사항을 구현하려면 변경 관리 시스템을 사용하여 변경 요청(RFC)을 생성해야 합니다. 보안 및 운영 팀이 사전 심사한 자동 변경 사항 라이브러리에서 RFCs를 생성하거나 AMS Advanced에서 안전하고 지원되는 것으로 간주되는 경우 운영 팀이 검토하고 구현하는 수동 변경을 요청합니다.

또한 AMS Advanced는 다양한 SLAs를 제공합니다. 자세한 내용은 [AWS Managed Services AMS Advanced 서비스 설명](#)을 참조하세요.

AWS Managed Services 시작하기

다중 계정 랜딩 존 AMS 서비스 시작에 대한 자세한 내용은 [AWS Managed Services 온보딩 소개를 참조하세요](#). 두 가지 온보딩 가이드는 서비스에 대한 설명과 시작하는 데 도움이 되도록 고려해야 할 질문을 제공합니다. [AWS Managed Services](#) 기능 세트와 [AWS Managed Services](#) 리소스의 현재 리소스를 검토합니다.

AMS 키 용어

- AMS Advanced: AMS Advanced 설명서의 "서비스 설명" 섹션에 설명된 서비스입니다. [서비스 설명](#)을 참조하세요.
- AMS 고급 계정: AWS AMS 고급 온보딩 요구 사항의 모든 요구 사항을 항상 충족하는 계정입니다. AMS Advanced 혜택, 사례 연구 및 영업 담당자에게 문의하는 방법에 대한 자세한 내용은 [AWS Managed Services](#)를 참조하세요.
- AMS Accelerate Accounts: AWS AMS Accelerate 온보딩 요구 사항의 모든 요구 사항을 항상 충족하는 계정입니다. [AMS Accelerate 시작하기를 참조하세요](#).
- AWS Managed Services: AMS 및 또는 AMS Accelerate.
- AWS Managed Services 계정: AMS 계정 및 또는 AMS Accelerate 계정.

- **중요 권장 사항:** 리소스 또는에 대한 잠재적 위험 또는 중단을 방지하기 위해 조치가 필요함을 알리는 서비스 요청을 AWS 통해에서 발급한 권장 사항입니다 AWS 서비스. 지정된 날짜까지 중요 권장 사항을 따르지 않기로 결정한 경우 결정으로 인한 모든 손해에 대한 책임은 전적으로 사용자에게 있습니다.
- **고객 요청 구성:** 다음에서 식별되지 않은 모든 소프트웨어, 서비스 또는 기타 구성:
 - Accelerate: [지원되는 구성](#) 또는 [AMS Accelerate, 서비스 설명](#).
 - AMS Advanced: [지원되는 구성](#) 또는 [AMS Advanced, 서비스 설명](#).
- **인시던트 통신:** AMS는 AMS Accelerate용 지원 센터와 AMS용 AMS 콘솔에서 생성된 인시던트를 통해 인시던트를 전달하거나 사용자가 AMS로 인시던트를 요청합니다. AMS Accelerate 콘솔은 대시보드의 인시던트 및 서비스 요청 요약과 자세한 내용은 지원 센터 링크를 제공합니다.
- **관리형 환경:** AMS Advanced 계정 및 또는 AMS에서 운영하는 AMS Accelerate 계정.

AMS Advanced의 경우 여기에는 다중 계정 랜딩 존(MALZ) 및 단일 계정 랜딩 존(SALZ) 계정이 포함됩니다.

- **결제 시작 날짜:**가 AWS Managed Services 온보딩 이메일에서 요청한 정보를 AWS 수신한 다음 영업일입니다. AWS Managed Services 온보딩 이메일은 계정에서 AWS Managed Services를 활성화하는 데 필요한 정보를 수집 AWS 하기 위해에서 사용자에게 보내는 이메일을 말합니다.

이후에 등록한 계정의 경우 청구 시작일은 AWS Managed Services가 등록된 계정에 대한 AWS Managed Services 활성화 알림을 보낸 다음 날입니다. AWS Managed Services 활성화 알림은 다음과 같은 경우에 발생합니다.

1. 호환되는 AWS 계정에 대한 액세스 권한을 부여하고 AWS Managed Services에 전달합니다.
 2. AWS Managed Services는 AWS Managed Services 계정을 설계하고 빌드합니다.
- **서비스 종료:** 서비스 요청을 통해 AWS 최소 30일 전에 알림을 제공하여 어떤 이유로든 AWS Managed Services 모든 AWS Managed Services 계정 또는 지정된 AWS Managed Services 계정에 대해 AWS Managed Services를 종료할 수 있습니다. 서비스 종료 날짜에 다음 중 하나를 수행합니다.
 1. AWS 모든 AWS Managed Services 계정 또는 해당하는 경우 지정된 AWS Managed Services 계정의 제어를 사용자에게 인계하거나
 2. 양 당사자는 해당하는 경우 모든 AWS Managed Services 계정 또는 지정된 AWS Managed Services 계정에서 AWS 액세스 권한을 부여하는 AWS Identity and Access Management 역할을 제거합니다.
 - **서비스 종료 날짜:** 서비스 종료 날짜는 30일의 필수 종료 알림 기간이 끝나는 달의 마지막 날입니다. 필수 종료 알림 기간이 해당 월의 20일 이후인 경우 서비스 종료 날짜는 다음 달의 마지막 날입니다. 다음은 종료 날짜에 대한 예제 시나리오입니다.

- 종료 알림이 4월 12일에 제공된 경우 30일 알림은 5월 12일에 종료됩니다. 서비스 종료 날짜는 5월 31일입니다.
- 종료 알림이 4월 29일에 제공된 경우 30일 알림은 5월 29일에 종료됩니다. 서비스 종료 날짜는 6월 30일입니다.
- AWS Managed Services:makes를 제공하면 서비스 시작 날짜부터 각 AWS Managed Services 계정에 대한 AWS Managed Services에 액세스하고 사용할 수 있습니다. AWS
- 지정된 AWS Managed Services 계정에 대한 종료: 서비스 요청("AMS 계정 종료 요청")을 통해 AWS 알림을 제공하여 어떤 이유로든 지정된 AWS Managed Services 계정에 AWS Managed Services 대한 AWS Managed Services를 종료할 수 있습니다.

인시던트 관리 용어:

- 이벤트: AMS 환경의 변경 사항입니다.
- 알림: 지원되는 이벤트가 임계값을 AWS 서비스 초과하고 경보를 트리거할 때마다 알림이 생성되고 연락처 목록으로 알림이 전송됩니다. 또한 인시던트 목록에 인시던트가 생성됩니다.
- 인시던트: AWS Managed Services 또는 사용자가 보고한 대로 영향을 미치는 AMS 환경 또는 AWS Managed Services의 예상치 못한 중단 또는 성능 저하입니다.
- 문제: 하나 이상의 인시던트에 대한 공유된 근본 원인입니다.
- 인시던트 해결 또는 인시던트 해결:
 - AMS가 해당 인시던트와 관련하여 사용할 수 없는 모든 AMS 서비스 또는 리소스를 사용 가능한 상태로 복원한 경우
 - AMS에서 사용할 수 없는 스택 또는 리소스를 사용 가능한 상태로 복원할 수 없다고 판단한 경우
 - AMS가 사용자가 승인한 인프라 복원을 시작했습니다.
- 인시던트 대응 시간: 인시던트를 생성하는 시점과 AMS가 콘솔, 이메일, 서비스 센터 또는 전화를 통해 초기 응답을 제공하는 시점 간의 시간 차이입니다.
- 인시던트 해결 시간: AMS 또는 사용자가 인시던트를 생성하는 시점과 인시던트가 해결되는 시점 간의 시간 차이입니다.
- 인시던트 우선 순위: AMS 또는 사용자가 인시던트의 우선 순위를 낮음, 중간 또는 높음으로 지정하는 방법입니다.
 - 낮음: AMS 서비스의 중요하지 않은 문제입니다.
 - 중간: 관리형 환경 내의 AWS 서비스를 사용할 수 있지만 의도한 대로 작동하지 않습니다(해당 서비스 설명에 따라).

- **높음:** (1) AMS 콘솔 또는 관리형 환경 내의 하나 이상의 AMS APIs를 사용할 수 없거나, (2) 관리형 환경 내의 하나 이상의 AMS 스택 또는 리소스를 사용할 수 없고 사용 불가능으로 인해 애플리케이션이 기능을 수행할 수 없습니다.

AMS는 위 지침에 따라 인시던트를 다시 분류할 수 있습니다.

- **인프라 복원:** 인시던트 해결이 불가능할 때 달리 지정하지 않는 한 영향을 받는 스택의 템플릿을 기반으로 기존 스택을 재배포하고 마지막으로 알려진 복원 지점을 기반으로 데이터 복원을 시작합니다.

인프라 용어:

- **관리형 프로덕션 환경:** 고객의 프로덕션 애플리케이션이 있는 고객 계정입니다.
- **관리형 비프로덕션 환경:** 개발 및 테스트용 애플리케이션과 같은 비프로덕션 애플리케이션만 포함하는 고객 계정입니다.
- **AMS 스택:** AMS에서 단일 단위로 관리하는 하나 이상의 AWS 리소스 그룹입니다.
- **변경 불가능한 인프라:** Amazon EC2 Auto Scaling 그룹(ASGs)에 일반적으로 사용되는 인프라 유지 관리 모델로, 업데이트된 인프라 구성 요소(AMI)는 현재 위치에서 업데이트되지 않고 모든 배포 AWS에 대해 대체됩니다. 변경 불가능한 인프라의 장점은 모든 구성 요소가 항상 동일한 기반에서 생성되므로 동기 상태를 유지하는 것입니다. 변형성은 AMI 구축을 위한 도구 또는 워크플로와 무관합니다.
- **변경 가능한 인프라:** Amazon EC2 Auto Scaling 그룹이 아니며 단일 인스턴스 또는 단 몇 개의 인스턴스를 포함하는 스택에 일반적으로 사용되는 인프라 유지 관리 모델입니다. 이 모델은 수명 주기가 시작될 때 시스템을 배포한 다음 시간이 지남에 따라 해당 시스템에 업데이트를 계층화하는 기존의 하드웨어 기반 시스템 배포를 가장 잘 나타냅니다. 시스템에 대한 모든 업데이트는 인스턴스에 개별적으로 적용되며 애플리케이션 또는 시스템 재시작으로 인해 시스템 가동 중지(스택 구성에 따라 다름)가 발생할 수 있습니다.
- **보안 그룹:** 인바운드 및 아웃바운드 트래픽을 제어하는 인스턴스의 가상 방화벽입니다. 보안 그룹은 서브넷 수준이 아니라 인스턴스 수준에서 작동하므로 따라서 VPC의 서브넷에 있는 각 인스턴스에는 서로 다른 보안 그룹 세트가 할당될 수 있습니다.
- **서비스 수준 계약(SLAs):** 예상 서비스 수준을 정의하는 AMS 계약의 일부입니다.
- **SLA 사용 불가 및 사용 불가:**
 - 오류가 발생하는 API 요청입니다.
 - 사용자가 제출한 콘솔 요청으로 5xx HTTP 응답이 발생합니다(서버가 요청을 수행할 수 없음).

- AMS 관리형 인프라에서 스택 또는 리소스를 구성하는 모든 AWS 서비스 오퍼링은 [서비스 상태 대시보드](#)에 표시된 대로 “서비스 중단” 상태입니다.
- AMS 제외로 인해 직접 또는 간접적으로 발생하는 사용 불가 서비스 크레딧 자격을 결정하는 데 고려되지 않습니다. 사용 불가 기준을 충족하지 않는 한 서비스는 사용 가능한 것으로 간주됩니다.
- 서비스 수준 목표(SLOs): AMS 서비스에 대한 특정 서비스 목표를 정의하는 AMS 계약의 일부입니다.

패치 용어:

- 필수 패치: 환경 또는 계정의 보안 상태를 손상시킬 수 있는 문제를 해결하기 위한 중요한 보안 업데이트입니다. ‘중요 보안 업데이트’는 AMS 지원 운영 체제의 공급업체가 ‘중요’로 평가한 보안 업데이트입니다.
- 발표된 패치와 릴리스된 패치: 패치는 일반적으로 일정에 따라 발표되고 릴리스됩니다. 발생한 패치는 패치의 필요성이 발견되면 발표되며, 일반적으로 패치가 릴리스된 직후 발표됩니다.
- 패치 추가 기능: AWS Systems Manager (SSM) 기능을 활용하는 AMS 인스턴스에 대한 태그 기반 패치를 제공하므로 인스턴스에 태그를 지정하고 구성한 기준 및 창을 사용하여 해당 인스턴스에 패치를 적용할 수 있습니다.
- 패치 방법:
 - 현재 위치 패치: 기존 인스턴스를 변경하여 수행되는 패치입니다.
 - AMI 대체 패치: 기존 EC2 Auto Scaling 그룹 시작 구성의 AMI 참조 파라미터를 변경하여 수행되는 패치입니다.
- 패치 공급자(OS 공급업체, 타사): 패치는 애플리케이션의 공급업체 또는 관리 기관에서 제공합니다.
- 패치 유형:
 - CSU(Critical Security Update): 지원되는 운영 체제의 공급업체가 "Critical"로 평가한 보안 업데이트입니다.
 - 중요 업데이트(IU): 지원되는 운영 체제의 공급업체가 “중요”로 평가한 보안 업데이트 또는 “중요”로 평가한 비보안 업데이트입니다.
 - 기타 업데이트(OU): CSU 또는 IU가 아닌 지원되는 운영 체제의 공급업체에 의한 업데이트입니다.
- 지원되는 패치: AMS는 운영 체제 수준 패치를 지원합니다. 보안 취약성 또는 기타 버그를 수정하거나 성능을 개선하기 위해 공급업체에서 업그레이드를 릴리스합니다. 현재 지원되는 OSs 목록은 [지원 구성을 참조하세요](#).

보안 용어:

- **탐지 제어:** 보안, 운영 또는 고객 제어와 일치하지 않는 구성에 대해 고객 관리형 환경 및 워크로드를 지속적으로 감독하고 소유자에게 알리거나 리소스를 사전에 수정 또는 종료하여 조치를 취하는 AMS 생성 또는 활성화된 모니터 라이브러리입니다.

서비스 요청 조건:

- **서비스 요청:** AMS가 사용자를 대신하여 수행할 작업에 대한 사용자의 요청입니다.
- **알림 알림:** AMS 알림이 트리거될 때 AMS가 서비스 요청 목록 페이지에 게시한 알림입니다. 계정에 대해 구성된 연락처도 구성된 메서드(예: 이메일)를 통해 알림을 받습니다. 인스턴스/리소스에 연락처 태그가 있고 태그 기반 알림에 대해 클라우드 서비스 제공 관리자(CSDM)에 동의를 제공한 경우 태그의 연락처 정보(키 값)에도 자동 AMS 알림에 대한 알림이 전송됩니다.
- **서비스 알림:** 서비스 요청 목록 페이지에 게시되는 AMS의 알림입니다.

기타 용어:

- **AWS Managed Services 인터페이스:** AMS의 경우: AWS Managed Services 고급 콘솔, AMS CM API 및 지원 API. AMS Accelerate의 경우: 지원 콘솔 및 지원 API.
- **고객 만족도(CSAT):** AMS CSAT는 모든 사례 또는 서신에 대한 사례 대응 등급, 분기별 설문 조사 등을 포함한 심층 분석을 통해 정보를 제공합니다.
- **DevOps:** DevOps는 모든 단계에서 자동화 및 모니터링을 강력하게 지원하는 개발 방법론입니다. DevOps는 자동화 기반을 통해 개발 및 운영의 기존 분리 기능을 결합하여 개발 주기를 단축하고, 배포 빈도를 늘리고, 보다 신뢰할 수 있는 릴리스를 목표로 합니다. 개발자가 운영을 관리할 수 있고 운영에서 개발을 알리면 문제와 문제가 더 빠르게 발견 및 해결되고 비즈니스 목표가 더 쉽게 달성됩니다.
- **ITIL: Information Technology Infrastructure Library(ITIL이라고 함)**는 IT 서비스의 수명 주기를 표준화하도록 설계된 ITSM 프레임워크입니다. ITIL은 서비스 전략, 서비스 설계, 서비스 전환, 서비스 운영, 서비스 개선 등 IT 서비스 수명 주기를 다루는 5단계로 구성됩니다.
- **IT 서비스 관리(ITSM):** IT 서비스를 비즈니스 요구 사항에 맞게 조정하는 일련의 사례입니다.
- **관리형 모니터링 서비스(MMS):** AMS는 자체 모니터링 시스템인 관리형 모니터링 서비스(MMS)를 운영합니다. 이 시스템은 AWS 상태 이벤트를 사용하고 Amazon CloudWatch 데이터 및 다른 데이터를 집계하여 Amazon Simple Notification Service(Amazon SNS) 주제를 통해 생성된 모든 경보를 AMS 운영자(온라인 24x7)에게 AWS 서비스 알림합니다.
- **네임스페이스:** IAM 정책을 생성하거나 Amazon 리소스 이름(ARNs)으로 작업할 때 네임스페이스 AWS 서비스를 사용하여 식별합니다. 작업 및 리소스를 식별할 때 네임스페이스를 사용합니다.

서비스 설명

AMS Advanced(AMS)는 AWS 인프라 운영을 관리하기 위한 AWS Managed Services 서비스의 운영 계획입니다. AMS Advanced는 패치, 연속성 관리, 보안 관리, 인시던트, 변경 및 서비스 요청 관리와 같은 IT 관리 프로세스와 같은 일상적인 인프라 작업을 제공합니다. 지원되는 서비스의 목록은 [지원되는 AWS 서비스](#) 단원을 참조하세요.

YouTube 동영상: [AMS가 클라우드에서 운영 우수성을 달성하는 데 어떻게 도움이 될 수 있나요?](#)

주제

- [AWS Managed Services\(AMS\) AMS Advanced 운영 계획 기능](#)
- [수행하는 작업, 수행하지 않는 작업](#)
- [AMS 책임 매트릭스\(RACI\)](#)
- [AMS 환경 기본 구성 요소](#)
- [AMS 계정 제한](#)
- [AMS 서비스 수준 목표\(SLOs\)](#)
- [지원되는 AWS 서비스](#)
- [지원되는 구성](#)
- [AMS에서 지원되지 않는 운영 체제의 기능](#)
- [AMS 고급 인터페이스](#)
- [AMS VPC 엔드포인트](#)
- [AMS 보호 네임스페이스](#)
- [AMS 예약 접두사](#)
- [AMS 유지 관리 기간](#)

AWS Managed Services(AMS) AMS Advanced 운영 계획 기능

AMS Advanced는 지원되는 AWS 서비스에 대해 다음과 같은 기능을 제공합니다.

- 로깅, 모니터링, 가드레일 및 이벤트 관리:

AMS는 활동 로깅을 위해 관리형 환경을 구성 및 모니터링하고 다양한 상태 확인을 기반으로 알림을 정의합니다. AMS는 해당 AWS 서비스에 대해 알림을 조사하며, 이러한 서비스 사용에 부정적인 영향을 미치는 알림은 인시던트를 생성합니다. AMS는 CloudWatch, CloudTrail CloudTrail의 모든 작업 및 Amazon S3의 시스템 로그의 결과로 생성된 모든 로그를 집계하고 저장합니다. 추가 알림을

설정하도록 요청할 수 있습니다. AMS의 예방 제어 외에도 AMS는 구성 가드레일과 탐지 제어를 배포하여 관리형 계정의 운영 및 보안 무결성을 저하시킬 수 있는 잘못된 구성으로부터 지속적으로 보호하여 태그 지정 및 규정 준수와 같은 제어를 적용합니다. 모니터링된 제어가 감지되면 경보가 생성되어 사용자가 수정할 수 있는 사전 정의된 AMS 기본값을 기반으로 리소스가 알림, 수정 또는 종료됩니다.

- 연속성 관리(백업 및 복원):

AMS는 사용자가 결정한 예약된 간격으로 표준 기존 AWS Backup 기능을 사용하여 리소스 백업을 제공합니다. 특정 스냅샷의 복원 작업은 AMS에서 RFC를 사용하여 수행할 수 있습니다. 스냅샷 간격 사이에 발생하는 데이터 변경은 백업에 대한 사용자의 책임입니다. 예약된 간격 외에 백업 또는 스냅샷 요청을 위해 RFC를 제출할 수 있습니다. AWS 리전에서 가용 영역(AZ)을 사용할 수 없는 경우 AMS는 사용자의 권한으로 영향을 받는 스택의 템플릿 및 사용 가능한 EBS 스냅샷을 기반으로 새 스택(들)을 다시 생성하여 관리형 환경을 복원합니다.

- 보안 및 액세스 관리:

AMS는 바이러스 백신 및 맬웨어 방지 보호 구성과 같은 엔드포인트 보안(EPS)을 제공합니다. 또한 자체 EPS 도구 및 프로세스를 사용할 수 있으며 자체 EPS 가져오기(BYOEPS)라는 기능을 사용하여 EPS용 AMS를 사용할 수 없습니다. 또한 AMS는 AWS Identity and Access Management (IAM) 역할 및 Amazon EC2 AWS 보안 그룹과 같이 온보딩 중에 사용자가 승인한 기본 보안 기능을 구성하고 표준 AWS 도구(예: AWS Security Hub Amazon Macie, Amazon GuardDuty)를 사용하여 보안 문제를 모니터링하고 대응합니다. 사용자가 제공한 승인된 디렉터리 서비스를 통해 사용자를 관리합니다. 승인된 디렉터리 서비스 목록은 섹션을 참조하세요 [지원되는 구성](#).

AMS에는 안티바이러스(AV)와 안티맬웨어 보호, 맬웨어 및 침입 탐지(Trend Micro)를 포함하는 엔드포인트 보안(EPS)이 포함됩니다. 보안 그룹은 스택 템플릿별로 정의되며 애플리케이션(퍼블릭/프라이빗) 보안 그룹의 가시성에 따라 시작 시 수정됩니다.

시스템에 대한 액세스는 변경 관리 요청(RFCs, 액세스 관리를 통해 Amazon EC2 인스턴스, AWS Management Console 및 APIs. AWS에 온보딩 및 페더레이션하는 동안 AMS Microsoft Active Directory 배포와 단방향 신뢰를 구축한 후에는 모든 상호 작용에 기존 회사 자격 증명을 사용할 수 있습니다.

- 패치 관리:

AMS는 지원되는 운영 체제(OSs) 및 지원되는 운영 체제가 사전 설치된 소프트웨어에 대해 EC2 인스턴스에 업데이트를 적용하고 설치합니다. 지원되는 운영 체제 목록은 섹션을 참조하세요 [지원되는 구성](#).

AMS는 패치를 위한 두 가지 모델을 제공합니다.

- 기존 계정 기반 패치를 위한 AMS 표준 패치 및
- AMS 패치 오케스트레이터, 태그 기반 패치용.

AMS 표준 패치에서는 AMS가 대부분의 패치 작업을 수행할 수 있도록 월별 유지 관리 기간이 선택됩니다. AMS는 선택한 유지 관리 기간(적절한 알림 포함) 외부에서 중요한 보안 업데이트와 선택한 유지 관리 기간 동안의 중요한 업데이트를 적용합니다. AMS는 선택한 유지 관리 기간 동안 인프라 관리 도구에 업데이트를 추가로 적용합니다. 원하는 경우 패치 관리에서 스택을 제외하거나 업데이트를 거부할 수 있습니다.

계정당 기본 유지 관리 기간인 AMS Patch Orchestrator를 사용하면 AMS가 패치 작업을 수행할 수 있도록 사용자가 정의합니다. AMS에 대한 추가 사용자 지정 유지 관리 기간을 예약하여 사용자가 정의한 특정 인스턴스 세트를 태그로 패치할 수 있습니다. AMS는 사용 가능한 모든 업데이트를 적용하지만 사용자 지정 패치 기준을 생성하여 업데이트를 필터링하거나 거부할 수 있습니다. 두 모델 모두 패치 관리에 제공된 업데이트를 승인하거나 거부했지만 나중에 마음이 바뀌는 경우 RFC를 통해 업데이트를 시작할 책임은 사용자에게 있습니다. AMS는 리소스의 패치 상태를 추적하고 월별 비즈니스 검토에서 최신이 아닌 시스템을 강조 표시합니다. 패치 관리는 모든 AMS 관리형 애플리케이션과 패치 기능이 있는 지원되는 AWS 서비스(예: RDS)를 포함하여 관리형 환경의 스택으로 제한됩니다. 업데이트가 릴리스될 때 모든 유형의 인프라 구성을 지원하기 위해 AMS a) EC2 인스턴스를 업데이트하고 b) 사용할 수 있는 업데이트된 AMS AMI를 제공합니다. 위에서 특별히 다루지 않은 추가 애플리케이션을 설치, 구성, 패치 및 모니터링하는 것은 사용자의 책임입니다.

- 변경 관리:

AMS 변경 관리는 관리형 환경의 변경 사항을 제어하는 메커니즘입니다. AMS는 예방 및 탐지 제어를 조합하여이 프로세스를 용이하게 하고 선택한 AMS 모드에 따라 다양한 수준의 제어 및 관련 위험을 제공합니다.

AMS 환경의 모든 작업이 로그인됩니다 AWS CloudTrail.

AMS 변경 관리 및 다양한 모드에 대한 자세한 내용은 [AMS 변경 관리 가이드](#) 및 [AMS 모드를 참조하세요](#).

- 자동 및 셀프 서비스 프로비저닝 관리:

다음과 같은 여러 가지 방법으로 AMS Advanced에서 AWS 리소스를 프로비저닝할 수 있습니다.

- 프로비저닝 및 구성 변경 요청(RFCs) 제출
- AWS Service Catalog를 통해 배포
- [Direct Change 모드](#)를 통해 배포

- [개발자 모드를](#) 통해 배포합니다. 개발자 모드를 통해 생성된 리소스는 AMS에서 관리하지 않습니다.
- 일부 AWS 서비스 에 대한 셀프 서비스 프로비저닝을 사용하여 AWS 서비스를 직접 구성합니다 (참조 [지원되는 AWS 서비스](#)).
- 인시던트 관리:

AMS는 AMS에서 감지한 인시던트를 사전에 알립니다. AMS는 고객이 제출한 인시던트와 AMS가 생성한 인시던트 모두에 응답하고 인시던트 우선 순위에 따라 인시던트를 해결합니다. 사용자가 달리 지시하지 않는 한, AMS에서 관리형 환경의 보안에 위협하다고 판단한 인시던트와 AMS 및 기타 AWS 서비스의 가용성과 관련된 인시던트는 사전에 조치를 취합니다. AMS는 권한이 부여되면 다른 모든 인시던트에 대해 조치를 취합니다. 반복되는 인시던트는 문제 관리 프로세스를 통해 해결됩니다.

- 문제 관리:

AMS는 추세 분석을 수행하여 문제를 식별 및 조사하고 근본 원인을 식별합니다. 문제는 해결 방법 또는 유사한 향후 서비스 영향의 재발을 방지하는 영구 솔루션으로 해결됩니다. 해결 시 "높음" 인시던트에 대해 사후 인시던트 보고서(PIR)를 요청할 수 있습니다. PIR은 근본 원인과 예방 조치 구현을 포함하여 취해진 예방 조치를 캡처합니다.

- 보고:

AMS는 실행 요약 및 인사이트, 운영 지표, 관리형 리소스, AMS 서비스 수준 계약(SLA) 준수, 지출, 절감 및 비용 최적화에 대한 재무 지표를 포함하여 AMS의 주요 성능 지표를 요약하는 월별 서비스 보고서를 제공합니다. 보고서는 사용자에게 할당된 AMS 클라우드 서비스 제공 관리자(CSDM)가 제공합니다.

- 서비스 요청 관리:

관리형 환경, AMS 또는 AWS 서비스 상품에 대한 정보를 요청하려면 AMS 콘솔을 사용하여 서비스 요청을 제출합니다. 서비스 및 기능에 대한 “방법” 질문에 대한 AWS 서비스 요청을 제출하거나 추가 AMS 서비스를 요청할 수 있습니다.

- 서비스 데스크:

AMS는 정규직 Amazon 직원과 엔지니어링 작업을 담당하여 인시던트 관리, 서비스 요청 관리 및 변경 관리를 포함한 비자동 요청을 이행합니다. 서비스 데스크는 연중무휴 운영됩니다.

- 지정된 리소스:

각 고객에게는 Cloud Service Delivery Manager(CSDM)와 Cloud Architect(CA)가 할당됩니다.

- CSDMs 직접 연락할 수 있습니다. 구현, 마이그레이션 및 운영 수명 주기의 모든 단계에서 서비스 검토, 제공 보고 및 인사이트를 수행합니다. CSDMs 월별 비즈니스 검토를 수행하고 재무 지출, 비용 절감 권장 사항, 서비스 사용률 및 위험 보고와 같은 항목을 자세히 설명합니다. 운영 성능 통계를 심층적으로 살펴보고 개선 영역에 대한 권장 사항을 제공합니다.
- CAs 직접 연락하여 AWS 클라우드 사용을 최적화하는 데 도움이 되는 기술 전문 지식을 제공할 수 있습니다. 예제 CA 활동에는 마이그레이션할 워크로드 선택, 추가 계정 및 워크로드 온보딩 지원, 게임 데이, 재해 복구 테스트, 문제 관리, AMS 미를 최대한 활용하기 위한 기술 조언과 같은 운영 활동의 기술적 리드 역할을 하는 것이 포함됩니다 AWS. CAs 조직의 모든 수준에서 기술 논의를 주도하고 인시던트 관리, 절충, 모범 사례 확립 및 기술 위험 완화를 지원합니다.

- 개발자 모드:

이 기능을 사용하면 AMS 변경 관리 프로세스에 대한 액세스 권한 외에도 AWS 서비스 APIs 및 AWS 콘솔에 대한 직접 액세스를 허용하여 AMS 구성 계정[1] 내에서 인프라 설계 및 배포를 빠르게 반복할 수 있습니다. 변경 관리 프로세스 외부에서 개발자 모드 권한으로 프로비저닝되거나 구성된 리소스는 관리할 책임이 있습니다("자동 및 셀프 서비스 프로비저닝 관리" 참조). AMS 변경 관리 프로세스를 통해 프로비저닝된 리소스는 AMS의 다른 변경 관리 프로비저닝 워크로드와 마찬가지로 지원됩니다.

- AWS 지원:

AMS 고객은 AMS 운영 계획을 보완하는 데 필요한 AWS Support 수준을 선택할 수 있습니다. AMS에 등록된 계정은 Business Support 또는 Enterprise Support를 구독할 수 있습니다. 지원 플랜의 차이점에 대해 알아보려면 [AWS 지원 플랜을 참조하세요](#).

- 고객 관리형 계정:

이 기능을 사용하면 동일한 관리형 환경 내에서 AWS 계정을 요청할 수 있지만 해당 계정 내에서 워크로드 및 AWS 리소스의 지속적인 운영은 사용자의 책임입니다. AMS는 고객 관리형 계정을 프로비저닝하지만 계정이 생성되면 해당 계정에 다른 AMS 기능 또는 서비스가 제공되지 않습니다. AWS는 고객 관리형 계정을 엔터프라이즈급 프리미엄 지원에 등록하지 않습니다. 선택한 지원 요금으로 AWS 지원에 고객 관리형 계정을 등록하는 것은 사용자의 책임입니다.

- 방화벽 관리:

AMS는 관리형 환경의 네트워크에 대한 인터넷 바운드 송신 트래픽 필터링을 지원하는 지원되는 방화벽 서비스를 위한 선택적 관리형 방화벽 솔루션을 제공합니다. AWS 네트워크 인프라를 사용하지 않고 트래픽이 인터넷으로 직접 전달되는 퍼블릭 서비스는 제외됩니다. 이 솔루션은 업계 최고의 방화벽 기술과 AMS 인프라 관리 기능을 결합하여 방화벽 인프라를 배포, 모니터링, 관리, 확장 및 복원합니다.

AMS를 온보딩하면 AMS 네트워크 인프라의 전체 목록을 받게 됩니다. 언제든지 AMS 인프라를 지원하기 위해 실행되는 서비스의 업데이트된 목록을 가져오려면 원하는 정보에 대한 세부 정보가 포함된 서비스 요청을 제출합니다. 네트워크 설계 변경을 요청하려면 VPC 추가 또는 보안 그룹 규칙 변경 요청과 같이 변경하려는 사항을 설명하는 서비스 요청을 생성합니다.

수행하는 작업, 수행하지 않는 작업

AMS는 AWS 인프라를 배포하는 표준화된 접근 방식을 제공하고 필요한 지속적인 운영 관리를 제공합니다. 역할, 책임 및 지원되는 서비스에 대한 전체 설명은 [서비스 설명](#)을 참조하세요.

Note

AMS가 추가 AWS 서비스를 제공하도록 요청하려면 서비스 요청을 제출합니다. 자세한 내용은 [서비스 요청하기를 참조하세요](#).

• 수행하는 작업:

온보딩을 완료하면 AMS 환경을 사용하여 변경(RFCs), 인시던트 및 서비스 요청에 대한 요청을 받을 수 있습니다. AMS 서비스와의 상호 작용은 애플리케이션 스택의 수명 주기를 중심으로 이루어집니다. 새 스택은 미리 구성된 템플릿 목록에서 정렬되고, 특정 Virtual Private Cloud(VPC) 서브넷으로 시작되며, 변경 요청(RFCs, 이벤트 및 인시던트가 연중무휴 모니터링됩니다.

활성 애플리케이션 스택은 패치 적용을 포함하여 AMS에서 모니터링 및 유지 관리되며 변경이 필요하거나 스택이 폐기되지 않는 한 스택 수명 동안 추가 작업이 필요하지 않습니다. 스택의 상태 및 기능에 영향을 미치는 AMS에서 감지한 인시던트는 알림을 생성하며 해결하거나 확인하기 위해 조치가 필요할 수도 있고 필요하지 않을 수도 있습니다. 서비스 요청을 제출하여 방법 질문 및 기타 문의를 할 수 있습니다.

또한 AMS를 사용하면 AMS에서 관리하지 않는 호환되는 AWS 서비스를 활성화할 수 있습니다. AWS-AMS 호환 서비스에 대한 자세한 내용은 [셀프 서비스 프로비저닝 모드를 참조하세요](#).

• 하지 말아야 할 일:

AMS는 다양한 수동 및 자동 옵션을 제공하여 애플리케이션 배포를 간소화하지만 애플리케이션의 개발, 테스트, 업데이트 및 관리는 사용자의 책임입니다. AMS는 애플리케이션에 영향을 미치는 인프라 문제에 대한 문제 해결 지원을 제공하지만 AMS는 애플리케이션 구성에 액세스하거나 검증할 수 없습니다.

AMS 책임 매트릭스(RACI)

Note

적시에 의무를 이행하기 위해 AWS Managed Services(AMS)는 적절한 조치를 결정하기 위해 사용자의 입력을 요구할 수 있습니다. AMS는 이러한 모든 설명 및 입력을 위해 지정된 고객 연락처에 문의합니다. AMS는 영업일 기준 24시간 이내에 이러한 쿼리에 응답할 것으로 예상합니다. 영업일 기준 24시간 이내에 응답이 없는 경우 AMS는 사용자를 대신하여 작업을 선택할 수 있습니다.

AMS 책임, 책임, 상담 및 정보 제공 또는 RACI 매트릭스는 다양한 활동에 대해 고객 또는 AMS에 기본 책임을 할당합니다.

AMS는 AWS 인프라를 관리합니다. 다음 표에는 AMS 관리형 환경 내에서 실행되는 애플리케이션의 수명 주기 활동에 대한 고객 및 AMS의 책임에 대한 개요가 나와 있습니다.

AMS는 고객 관리형 계정 또는 계정 내에서 실행되는 인프라에 대한 다음 활동에 대해 책임을 지지 않으므로 이 RACI는 적용되지 않습니다.

- R은 작업을 수행하기 위해 작업을 수행하는 책임 당사자를 나타냅니다.
- C는 컨설팅, 일반적으로 주제 전문가로서 의견을 구하는 당사자, 양자 간 커뮤니케이션이 있는 당사자를 의미합니다.
- 나는 정보, 즉 종종 작업 또는 결과물 완료 시에만 진행 상황에 대한 정보를 받는 당사자를 의미합니다.
- 셀프 서비스 프로비저닝은 개발자 모드 및 셀프 서비스 프로비저닝된 서비스를 포함하여 AWS API 또는 콘솔을 통해 셀프 서비스를 통해 고객이 프로비저닝한 리소스를 말합니다.

Note

일부 섹션에는 AMS와 고객 모두에 대한 'R'이 포함되어 있습니다. 공동 AWS 책임 모델에서 AMS와 고객 모두 공동 소유권을 가지고 인프라 및 애플리케이션 문제에 대응하기 때문입니다.

셀프 서비스 프로비저닝 기능을 제공하기 위해 AMS는 권한 경계가 있는 승격된 IAM 역할을 생성하여 직접 AWS 서비스 액세스에서 의도하지 않은 변경을 제한했습니다. 역할은 모든 변경 사항을 방

지하지 않으며 내부 제어, 규정 준수를 준수하고 사용 중인 모든 AWS 서비스가 필수 인증을 충족하는지 확인할 책임이 있습니다. 이를 셀프 서비스 프로비저닝 모드라고 합니다. AWS 규정 준수 요구 사항에 대한 자세한 내용은 [AWS 규정](#) 준수를 참조하세요.

셀프 서비스를 통해 프로비저닝하는 리소스의 경우 AMS는 서비스 요청을 통해 인시던트 관리, 탐지 제어 및 가드레일, 보고, 지정된 리소스(Cloud Service Delivery Manager 및 Cloud Architect), 보안 및 액세스, 기술 지원을 제공합니다. 또한 해당하는 경우 AMS 변경 관리 시스템 외부에서 프로비저닝되거나 구성된 리소스의 연속성 관리, 패치 관리, 인프라 모니터링 및 변경 관리에 대한 책임을 집니다.

활동	Customer	AWS Managed Services(AMS)
애플리케이션 수명 주기		
애플리케이션 개발	R	정보
애플리케이션 인프라 요구 사항 분석 및 설계	R	C
비표준 AMS 스택을 위한 설계 및 최적화	R	C
AMS 표준 스택의 설계 및 최적화	정보	R
애플리케이션 배포	R	C
AWS 인프라 배포	C	R
애플리케이션 모니터링	R	정보
애플리케이션 테스트/최적화	R	정보
AWS 인프라 최적화 지침	정보	R
AWS 인프라 모니터링	정보	R
애플리케이션 문제 해결	R	C
AWS 네트워크 문제 해결	C	R
운영 체제 및 인프라 문제 해결	C	R

활동	Customer	AWS Managed Services(AMS)
셀프 서비스 프로비저닝	R	C
애플리케이션 및 ITSM 통합		
AWS Service Offerings와의 애플리케이션 통합	R	C
AWS Managed Services 인터페이스와 ITSM 통합	R	C
네트워킹		
관리형 환경 VPC 및 VPC 설정 및 구성	C	R
VPCs에 프라이빗 주소 공간 할당(예: /16)	R	C
AWS가 아닌 AWS Managed Services, 고객 관리형 Firewalls/Proxy/Bastions/HOSTs 구성 및 운영	R	C
관리형 환경 내에서 AWS 보안 Groups/NAT/Customer Bastions/NACL 구성 및 운영	정보	R
고객 네트워크 내 네트워킹(예: DirectConnect) 구성 및 구현	R	C
관리형 환경 내 네트워킹 구성 및 구현	C	R
관리형 환경 구성		
기준 스택 템플릿에 대한 기본 Auto Scaling 설정 정의	정보	R
RI 최적화 권장	C	R
RI 및 PIOP 용량 구매	R	C
용량이 과다 프로비저닝될 때 용량 제거(고객 애플리케이션에서 지원하는 경우)	C	R

활동	Customer	AWS Managed Services(AMS)
AWS Managed Services에 대한 AWS 고객별 정보 생성/업데이트	C	R
S3 구성	C	R
셀프 서비스 프로비저닝	R	C
Glacier 구성	C	R
아카이브 정책 정의	R	C
아카이브 정책 구성	C	R
고객 유지 관리 기간 선택	R	정보
AWS RDS 관리		
source/replica/RO 복제 상태 모니터링	정보	R
소스 장애 조치의 RCA 식별	정보	R
자동 스냅샷(백업) 구성	C	R
셀프 서비스 프로비저닝	R	C
DB 엔진 패치 관리 조정 및 예약	C	R
셀프 서비스 프로비저닝	R	C
DB 스토리지 및 PIOP 용량 권장	C	R
셀프 서비스 프로비저닝	R	C
데이터베이스 실행을 위한 인스턴스 크기 조정 권장	C	R
셀프 서비스 프로비저닝	R	C

활동	Customer	AWS Managed Services(AMS)
관리형 환경을 위한 RI 최적화 권장	C	R
셀프 서비스 프로비저닝	R	C
RDS 성능 모니터링(CloudWatch)	C	R
셀프 서비스 프로비저닝	R	C
RDS 이벤트 구독 구성(SNS)	C	R
셀프 서비스 프로비저닝	R	C
RDS 보안 그룹 구성	C	R
셀프 서비스 프로비저닝	R	C
RDS 엔진 파라미터/옵션 구성	R	C
DB 테이블 설계	R	정보
DB 인덱싱	R	정보
DB 로그 분석	R	정보
AMS 변경 관리		
고객 RFCs 생성(예: 관리creating/updating/deleting 리소스에 대한 액세스, 애플리케이션 배포/업데이트, AWS 서비스 상품 구성 변경)	R	정보
고객 RFCs 승인	정보	R
AWS Managed Services RFCs 생성(예: 리소스에 대한 액세스, 고객을 대신하여 리소스 생성, 패치 관리의 일부로 OS에 업데이트 적용)	정보	R
비자동 RFCs 승인	R	정보

활동	Customer	AWS Managed Services(AMS)
새 변경 유형에 대한 요청 제출	R	C
새 변경 유형 생성	정보	R
애플리케이션 변경 일정 유지 관리	R	C
예정된 유지 관리 기간 알림	정보	R
AWS Service Catalog		
포트폴리오 및 제품 생성	R	정보
최종 사용자에게 제품 배포	R	정보
태그 및 태그 옵션 라이브러리 생성	R	C
최종 사용자와 포트폴리오 및 제품 공유	R	정보
포트폴리오 및 제품 수정/업데이트	R	정보
포트폴리오 및 제품에 제약 조건 생성 및 할당	R	C
제품에 서비스 작업 연결	R	C
프로비저닝된 리소스를 새 버전의 제품으로 업데이트	R	정보
프로비저닝		
AWS Managed Services 기준 AMI에 대한 고객 별 추가 사항	R	C
스택 템플릿을 프로비저닝하는 데 사용되는 승인된 추가 변경 유형 구성	C	R

활동	Customer	AWS Managed Services(AMS)
AMS 변경 관리 프로세스 또는 AWS Service Catalog를 통해 제출된 관리형 스택 및 관련 AWS 리소스를 시작합니다.	정보	R
	R	정보
셀프 서비스 프로비저닝		
AMS 변경 관리 프로세스 또는 AWS Service Catalog를 통해 프로비저닝된 인스턴스에 사용자 지정 및 타사 애플리케이션을 설치/업데이트합니다.	R	정보
프로비저닝 - 스택 아키텍처		
OS 라이선스 제공(해당 AWS 서비스에 대한 사용 요금 포함 - 예: EC2 및 RDS)	정보	R
	R	I
셀프 서비스 프로비저닝		
AMS 변경 관리 시스템을 통해 애플리케이션 배포를 위한 기본 인프라 템플릿(Stacks)을 정의합니다.	정보	R
	R	I
셀프 서비스 프로비저닝		
기준선 승인 AMIs 생성 ⁸	정보	R
고객 애플리케이션 인벤토리를 평가하고 사용할 가능한 인프라 템플릿(Stacks)에 적합한지 확인	R	C
기준 템플릿 오퍼링 외에 고유한 스택 정의	R	C
로깅, 모니터링 및 이벤트 관리		
AWS 인프라 변경 로그 기록	정보	R
모든 애플리케이션 변경 로그 기록	R	C

활동	Customer	AWS Managed Services(AMS)
AMS 변경 관리 프로세스를 통해 프로비저닝된 AWS 인프라의 패치 적용, 보안, 모니터링 등을 위한 에이전트 및 스크립트의 설치 및 구성.	정보	R
	R	C
셀프 서비스 프로비저닝		
고객별 모니터링 및 인시던트 요구 사항 정의	R	C
관리형 환경에 대한 알림 구성	정보	R
모든 AMS 구성 알림 모니터링	정보	R
셀프 서비스 프로비저닝	R	C
인시던트 알림을 위한 인프라 알림 조사	정보	R
셀프 서비스 프로비저닝	R	C
애플리케이션 경보 조사	R	C
인시던트 관리		
모니터링을 기반으로 AWS 인프라의 인시던트에 사전 알림	정보	R
	R	C
셀프 서비스 프로비저닝		
애플리케이션 성능 문제 및 중단 처리	R	정보
인시던트 우선순위 분류	정보	R
인시던트 대응 제공	정보	R

활동	Customer	AWS Managed Services(AMS)
인시던트 해결/인프라 복원 제공	C	R
Note SLAs는 셀프 서비스 프로비저닝 및 개발자 모드를 사용하여 프로비저닝된 리소스를 포함하여 AMS 변경 관리 외부에서 프로비저닝된 인스턴스 기반 리소스에는 적용되지 않습니다.		
문제 관리		
관리형 환경에서 문제 식별	C	R
관리형 환경에서 문제에 대한 RCA 수행	C	R
관리형 환경의 문제 해결	C	R
애플리케이션 문제 식별 및 해결	R	정보
보안 관리		
고객 온보딩 중에 결정되고 합의된 고객 인프라 보안 및/또는 보안 규정 준수 프로세스의 기준 설정.	C	R
	R	C
셀프 서비스 프로비저닝		
관리형 EPS에 유효한 라이선스 유지	R	C
관리형 EPS 구성	정보	R
셀프 서비스 프로비저닝	R	C
관리형 EPS 업데이트	정보	R
셀프 서비스 프로비저닝	R	C

활동	Customer	AWS Managed Services(AMS)
AMS CM 프로세스를 통해 프로비저닝된 인스턴스에서 맬웨어 모니터링.	정보	R
셀프 서비스 프로비저닝	R	C
바이러스 서명 유지 관리 및 업데이트.	정보	R
셀프 서비스 프로비저닝	R	C
맬웨어에 감염된 인스턴스 문제 해결.	C	R
셀프 서비스 프로비저닝	R	C
보안 이벤트 관리	C	R
보안 - 액세스 관리		
사용자의 수명 주기와 AWS Managed Services에 액세스하는 데 사용되는 로컬 디렉터리 서비스에 대한 권한을 관리합니다.	R	정보
AWS 콘솔/APIs에 대한 고객 액세스를 위해 페더레이션 인증 시스템(들) 운영	R	C
AWS Managed Services AD에서 고객 관리형 AD로의 Active Directory(AD) 신뢰 수락 및 유지	R	C
온보딩 중에 각 관리형 계정 내에서 교차 계정 IAM 관리자 역할을 생성합니다.	R	C
각 계정의 AWS 루트 자격 증명 보호	정보	R
관리형 환경을 위한 IAM 리소스 정의	C	R
AMS 엔지니어의 OS 액세스를 위한 권한 있는 자격 증명 관리	정보	R

활동	Customer	AWS Managed Services(AMS)
AMS에서 고객에게 제공하는 OS 액세스에 대한 권한 있는 자격 증명 관리	R	정보
보안 인시던트 대응 - 준비		
통신		
AMS가 보안 이벤트 알림 및 보안 에스컬레이션 중에 사용할 수 있도록 고객 보안 연락처 세부 정보 제공	R	정보
보안 이벤트 및 보안 에스컬레이션 중에 사용할 제공된 고객 보안 연락처 세부 정보를 저장하고 관리합니다.	CI	R
훈련		
인시던트 대응 프로세스 중에 AMS를 지원하는 설명서를 고객에게 제공	정보	R
보안 게임데이를 통해 인시던트 대응 프로세스 중에 공동 책임 연습	RI	RC
리소스 관리		
알림, 알림 상관 관계, 노이즈 감소 및 추가 규칙에 AWS 서비스 대해 지원되는 보안 관리 구성	정보	R
자산(AWS 리소스) 인벤토리를 유지하고 자산의 가치 및 중요도를 파악합니다. 이 정보는 인시던트 억제 전략 중에 유용합니다.	R	CI
AWS 태그를 사용하여 리소스 및 워크로드 식별	R	CI
로그 보존 및 아카이브 정의 및 구성	CI	R

활동	Customer	AWS Managed Services(AMS)
구성 AWS 계정, 정책 및 액세스 관리의 보안 기준 설정	CI	RC
보안 인시던트 대응 - 탐지		
로깅, 지표 및 모니터링		
인스턴스 및 계정에 대한 이벤트 관리를 활성화 하도록 로깅 및 모니터링 구성	CI	R
보안 알림 AWS 서비스 에 지원되는 모니터	정보	R
엔드포인트 보안 도구 배포 및 관리	CI	R
AMS 지원 엔드포인트 보안 도구를 사용하여 인스턴스에서 맬웨어 모니터링	정보	R
아웃바운드 메시징을 통해 감지된 이벤트를 고객에게 알림	정보	R
인시던트 대응 시간을 개선하기 위해 특정 계정 및 워크로드에 대한 의사 결정자에게 알림 및 후속 업데이트를 라우팅합니다.	R	CI
AMS 표준 탐지 서비스 정의, 배포 및 유지 관리 (예: Amazon GuardDuty 및 AWS Config)	CI	R
AWS 인프라 변경 로그 기록	정보	RC
로깅 활성화 및 구성, 애플리케이션에 대한 이벤트 관리를 활성화하기 위한 모니터링	R	C
지원되는 AWS 보안 서비스(예: Amazon GuardDuty)에 대한 허용 목록, 거부 목록 및 사용자 지정 탐지 구현 및 유지 관리	RCI	R
보안 이벤트 보고		

활동	Customer	AWS Managed Services(AMS)
AMS에 의심스러운 활동 또는 활성 보안 조사 알림	R	CI
감지된 보안 이벤트 및 인시던트를 고객에게 알림	정보	R
보안 인시던트 대응 프로세스를 트리거할 수 있는 계획된 이벤트에 알림	R	CI
보안 인시던트 대응 - 분석		
조사 및 분석		
지원되는 탐지 소스에서 생성된 지원되는 보안 알림에 대한 초기 응답 수행	정보	RC
사용 가능한 데이터를 사용하여 거짓/참 긍정 평가	RI	RC
필요한 경우 고객과 공유할 영향을 받는 인스턴스의 스냅샷 생성	정보	R
관리 연속성, 파일 시스템 분석, 메모리 포렌식 및 바이너리 분석과 같은 포렌식 작업 수행	R	CI
조사를 지원하는 애플리케이션 로그 수집	R	정보
데이터 및 로그를 수집하여 보안 알림에 대한 조사 지원	RCI	RC
보안 조사에 AWS 서비스 내 SMEs 참여	CI	R
조사 중에 타사 공급업체 참여(예: EPS 맬웨어 방지 조사 및 TrendMicro 지원 팀 참여)	RCI	정보
조사 중에 지원되는의 조사 로그 AWS 서비스를 고객에게 공유	정보	R

활동	Customer	AWS Managed Services(AMS)
통신		
관리형 리소스에 대한 AMS 탐지 소스의 알림 및 알림 전송	정보	R
애플리케이션 보안 이벤트에 대한 알림 및 알림 관리	R	정보
보안 인시던트 조사 중에 고객 보안 연락 담당자 참여	R	정보
보안 인시던트 대응 - 포함		
억제 전략 및 실행		
합의된 억제 전략의 실행을 결정하고 억제 기간 동안 서비스 가용성에 영향을 미칠 수 있는 결과에 합의합니다.	R	CI
추가 분석을 위해 영향을 받는 시스템을 백업합니다.	CI	R
애플리케이션 및 워크로드 포함(애플리케이션별 구성 또는 응답 활동을 통해)	R	CI
보안 인시던트 및 영향을 받는 리소스를 기반으로 억제 전략 정의	CI	R
영향을 받는 시스템의 특정 시점 백업에 대한 암호화 및 보안 저장 활성화	CI	R
EC2 인스턴스, 네트워크 및 IAM을 포함한 AWS 리소스에 대해 지원되는 격리 작업 실행	CI	R
보안 인시던트 대응 - 제거		
근절 전략 및 실행		

활동	Customer	AWS Managed Services(AMS)
고객 애플리케이션 워크로드에서 보안 인시던트 및 영향을 받는 리소스를 기반으로 근절 옵션 정의	R	CI
합의된 근절 전략, 근절 실행 시기 및 결과를 결정합니다.	R	CI
AMS 관리형 워크로드에서 보안 인시던트 및 영향을 받는 리소스를 기반으로 근절 단계 정의	CI	R
EC2 인스턴스, 네트워크 및 IAM 근절을 포함한 AWS 리소스 근절 및 강화	CI	R
애플리케이션 및 워크로드 제거 및 강화(애플리케이션별 구성 또는 응답 활동을 통해)	R	정보
보안 인시던트 대응 - 복구		
복구 준비 및 실행		
고객의 요청에 따라 백업 계획 및 대상 구성	R	정보
백업 계획을 검토하여 AMS 관리형 워크로드 복원	CI	R
지원되는 리소스에 대한 백업 복원 활동 수행 AWS 서비스	정보	R
고객 애플리케이션, APP 구성 및 배포 설정을 백업하고 백업 계획을 검토하여 인시던트 발생 후 고객 애플리케이션 및 워크로드를 복원합니다.	R	정보
애플리케이션 및 고객 워크로드 복원(애플리케이션별 복원 단계를 통해)	R	정보
보안 인시던트 대응 - 인시던트 사후 보고서		

활동	Customer	AWS Managed Services(AMS)
인시던트 사후 보고		
필요에 따라 고객 사후 인시던트와 적절한 교훈 및 조치 항목을 공유합니다.	정보	R
패치 관리 ⁹		
지원되는 OS 및 EC2 인스턴스용 지원되는 OS가 사전 설치된 소프트웨어에 해당하는 업데이트가 있는지 모니터링합니다.	정보	R
	R	C
셀프 서비스 프로비저닝		
고객에게 예정된 업데이트 알림(AMS 표준 패치에만 해당)	정보	R
패치 적용 활동에서 특정 업데이트 및/또는 특정 스택 제외	R	정보
패치(AMS 패치에 적용)를 적용할 기본 및 사용자 지정 유지 관리 기간 일정과 기타 파라미터(예: 유지 관리 기간 기간) 정의	R	정보
오케스트레이터만 해당)		
특정 패치를 필터링하고 제외할 사용자 지정 패치 기준 정의(AMS 패치 오케스트레이터에만 해당)	R	정보
인스턴스에 태그를 지정하여 사용자 지정 유지 관리 기간 및 패치 기준과 연결(AMS 패치 오케스트레이터에만 해당)	R	정보
리소스의 패치 상태를 추적하고 월별 비즈니스 검토에서 최신이 아닌 시스템을 강조 표시합니다.	C	R

활동	Customer	AWS Managed Services(AMS)
Windows 운영 체제 및 Windows Update에서 관리하는 운영 체제에 설치된 Microsoft 패키지 패치	정보	R
셀프 서비스 프로비저닝	R	-
Windows Update에서 관리하지 않는 패치 설치 애플리케이션, 소프트웨어 또는 애플리케이션 종속성	R	정보
셀프 서비스 프로비저닝	R	-
Linux 운영 체제 및 운영 체제의 기본 패키지 관리자(예: Yum, Apt, Zypper)에 의해 관리가 활성화된 모든 패키지에 패치 적용	정보	R
셀프 서비스 프로비저닝	R	-
Linux 운영 체제의 기본 패키지 관리자에서 관리하지 않는 패치 설치 애플리케이션, 소프트웨어 또는 애플리케이션 종속성	R	정보
셀프 서비스 프로비저닝	R	-
연속성 관리		
백업 일정 지정	R	정보
일정에 따라 백업을 실행합니다.	정보	R
셀프 서비스 프로비저닝	R	C
백업 검증	R	정보
백업 복원 활동 요청	R	정보

활동	Customer	AWS Managed Services(AMS)
백업 복원 활동을 실행합니다.	정보	R
셀프 서비스 프로비저닝	R	C
영향을 받는 스택 및 VPCs.	정보	R
셀프 서비스 프로비저닝	R	C
영향을 받는 사용자 지정/타사 애플리케이션 복원	R	C
보고		
월별 서비스 보고서 준비 및 전달	정보	R
의 AMS AWS Outposts	R	정보
온디맨드 API 감사 기록(CloudTrail)을 구성하고 검색합니다.	정보	R
셀프 서비스 프로비저닝	R	정보
AWS Managed Services Interface를 통해 인스턴트 기록에 대한 액세스 제공	정보	R
AWS Managed Services Interface를 통해 변경 기록에 대한 액세스 권한을 제공합니다.	정보	R
	N/A	N/A
셀프 서비스 프로비저닝		
서비스 요청 관리		
서비스 요청을 사용하여 정보 요청	R	정보
서비스 요청에 회신	정보	R
관리형 방화벽		

활동	Customer	AWS Managed Services(AMS)
AMS 관리형 방화벽 배포 요청	R	정보
AMS 관리형 방화벽 아키텍처의 설계 및 최적화	정보	R
AWS 인프라 및 AMS 관리형 방화벽 어플라이언스 배포	정보	R
방화벽 라이선스 제공(해당 AWS 서비스에 대한 사용 요금 포함 - 예: EC2)	R	정보
기본 도메인 허용 목록 정의	정보	R
사용자 지정 허용 목록 및 보안 정책 추가, 수정 및 삭제 요청	R	정보
AMS 관리형 방화벽에 대한 알림 구성	정보	R
모든 AMS 관리형 방화벽 구성 알림 모니터링	정보	R
방화벽 구성의 백업 실행	정보	R
백업 복원 활동 요청	R	정보
프로비저닝된 리소스를 새 버전의 제품으로 업데이트	정보	R
AMS 관리형 방화벽 로그 기록	정보	R
AMS 관리형 방화벽에서 CloudWatch로 로그 전달	정보	R
AMS 관리형 방화벽에서 구성 변경 요청	R	정보
AMS 관리형 방화벽에서 구성 변경 승인	정보	R
AMS 관리형 방화벽에서 구성 변경 실행	정보	R

⁸AMS는 Amazon EC2용 AMIs만 제공합니다.

⁹AMS는 고객이 OSES 공급업체와 추가 지원 계약에 서명하는 경우에만 수명 종료 OS에 대한 책임이 있습니다.

AMS 환경 기본 구성 요소

Multi-Account Landing Zone

코어 계정의 인프라 구성 요소 및 잠재적 비용을 추정한 것입니다. 여기에는 대역폭, CloudWatch 세부 모니터링, 로깅, 경보, Route53, Amazon S3, Simple Notification Service(Amazon SNS), 스냅샷 또는 예약된 Amazon EC2 인스턴스와 같은 기타 비용은 포함되지 않습니다.

AMS 관리형 AWS 랜딩 존 인프라에 필요한 구성 요소에 대해 비용을 지불합니다. 견적은 일반 AMS 다중 계정 랜딩 존 환경의 비용을 매월 2,450 USD, 일반 애플리케이션 계정의 경우 50 USD로 책정합니다.

요금에 대한 자세한 내용은 [AWS 요금](#)을 참조하세요.

기본 환경 구성 요소

구성 요소	Est. 비용	설명
관리 계정	60 USD	AWS Organizations Management 계정. 멤버 계정을 생성하고 재무적으로 관리합니다. 여기에는 AWS Landing Zone(ALZ) 프레임워크, 계정 구성 스택 세트 및 AWS Organization Service Control Policy(SCPs 포함됩니다. • 디렉터리 서비스: 35 USD • CloudTrail: 7 USD • CloudWatch: 6 USD • 기타: 12 USD
공유 서비스 계정	2000 USD	액세스 관리(예: Active Directory), 엔드포인트 보안 관리(Trend Micro) 및 접속(SSH/RDP)에 필요한 인프라와 리소스가 포함되어 있습니다. 추정치는 매월 2,400 USD입니다. 이 견적에는 Trend Micro 라이선스 비용이 포함되지 않습니다. • EC2: \$800(최소 Bastions 수 포함)

구성 요소	Est. 비용	설명
		• RDS: 300 USD(EPS) • VPC(엔드포인트): 400 USD • 디렉터리 서비스: 300 USD • CloudWatch: 100 USD • GuardDuty: 15 USD • Secrets Manager: 10 USD • 데이터 전송: 10 USD • 구성: 10 USD • 기타: 45 USD
네트워킹 계정	350 USD	AMS 계정 간 네트워크 라우팅, 온프레미스 네트워크 및 인터넷으로의 송신 트래픽을 위한 중앙 허브입니다. 또한에는 퍼블릭 DMZ 접속(AMS 엔지니어가 AMS 환경의 호스트에 액세스할 수 있는 진입점)이 포함되어 있습니다. Transit Gateway 및 Direct Connect를 통과하는 트래픽에 따라 가격이 증가할 수 있습니다. • EC2: 250 USD(배스션) • VPC: 80 USD • 기타: 20 USD
로그 아카이브 계정	20 USD	각 AMS 환경 계정의 AWS CloudTrail 및 AWS Config 로그 파일 사본이 있는 S3 버킷입니다. 더 많은 로그가 수집되면 비용이 증가합니다. • S3: 10 USD • CloudWatch: 5 USD • 기타: 5 USD

구성 요소	Est. 비용	설명
보안 계정	20 USD	보안 관련 작업을 위한 중앙 허브이자 AMS 컨트롤 플레인 서비스에 알림 및 알림을 퍼널링하기 위한 주요 지점입니다. 또한 예는 Amazon Guard Duty 관리 계정이 있습니다. Amazon GuardDuty를 사용하여 더 많은 이벤트를 분석하면 비용이 증가합니다. • CloudWatch: 15 USD • 기타: 5 USD

Single-Account Landing Zone

다음 표에는 예제 AMS 관리형 인프라의 구성 요소가 나열되어 있습니다.

기본 환경 구성 요소, 최종 업데이트 날짜 2020/07/09

이름	인스턴스 유형	OS	구성 요소 수
mc-eps-dsm	m5.large	Linux	2
mc-관리	m5.large	Windows	2
mc-bastion-dmz-ssh	m5.large	Linux	2
mc-bastion-customer-rdp	m5.large	Windows	2
mc-eps-relay	m5.large	Linux	2
디렉터리 서비스	N/A	N/A	
추가 구성 요소	N/A	N/A	

요금에 대한 자세한 내용은 [AWS 요금을](#) 참조하세요.

AMS 계정 제한

AMS 다중 계정 랜딩 존에는 AMS API 제한, AMS 리소스 제한 및 AWS 제한의 세 가지 고유한 제한 유형이 있습니다.

AMS 단일 계정 랜딩 존 내에서 고려해야 할 제한에는 AMS API 제한과 AWS 제한이라는 두 가지 유형이 있습니다.

AMS 계정 API 제한

이 섹션에서는 AWS Managed Services(AMS)가 AMS SKMS API 서비스를 제한하는 계정 수준 제한에 대해 설명합니다. 즉, 나열된 APIs를 1초에 10회 이상 호출하면 호출 중 하나가 "제한"됩니다(가수신됨ThrottleException). 드문 경우지만 외부 또는 다운스트림 종속성이 AMS API를 제한한 다음 AMS가 API 호출을 더 낮은 속도로 제한할 수 있습니다.

Note

AMS SKMS API에 대한 자세한 내용은 AWS Artifact 콘솔의 보고서 탭을 통해 참조를 다운로드하세요.

나열된 각 AMS SKMS API에 대해 작업은 10TPS(초당 트랜잭션) 후에 조절됩니다.

- GetStack
- GetSubnet
- GetVpc
- ListAmis
- ListStackSummaries
- ListSubnetSummaries
- ListVpcSummaries

AMS 다중 계정 랜딩 존 계정 리소스 제한

계정 리소스 제한은 AMS 다중 계정 랜딩 존 애플리케이션 계정 및 VPCs 및 서브넷과 관련이 있습니다.

애플리케이션 계정 리소스 제한

조직당 애플리케이션 계정은 50개로 소프트웨어 제한이 있습니다. 50개 이상의 애플리케이션 계정에 대한 사용 사례가 있는 경우 클라우드 서비스 제공 관리자(CSDM)에 문의하여 요구 사항을 전달합니다.

VPCs 및 서브넷 리소스 제한

조직의 사전 정의된 AWS 리전 내에서 애플리케이션 계정당 VPCs는 10개로 소프트웨어 제한이 있습니다.

각 VPC에는 2~3개의 가용 영역에 걸쳐 1~10개의 프라이빗 서브넷 티어가 있을 수 있습니다. 또한 각 VPC에는 2~3개의 가용 영역에 걸쳐 0~5개의 퍼블릭 서브넷 티어가 있을 수 있습니다. 이러한 한도를 초과하는 요구 사항이 있는 경우 CSDM 또는 Cloud Architect에 문의하여 사용 사례를 검토하세요.

AMS 다중 계정 랜딩 존 애플리케이션과 계정 비용

애플리케이션당 하나의 계정이 AMS 다중 계정 랜딩 존에서 지원되지만, 각 애플리케이션 계정에는 적은 비용이 발생하며 시간당 Transit Gateway에 대한 연결 수와 AWS Transit Gateway를 통해 흐르는 트래픽 양에 대해 요금이 부과됩니다. 따라서 애플리케이션이 계정 또는 VPCs로 더 많이 분리될수록 비용이 증가합니다.

비용을 절감하고 여전히 적절한 업무 분리를 보장하기 위해 AMS는 1) 비즈니스 프로세스가 긴밀하게 연결된 팀별로 애플리케이션을 그룹화하고 2) 다른 단계(생산 대 비생산)에 있거나 다른 팀에서 관리하는 애플리케이션을 혼합하지 않을 것을 권장합니다. 이렇게 하면 계정이 줄어들고 액세스 관리 및 업무 분리가 더 쉬워지며 트래픽 비용이 완화될 수 있습니다.

예를 들어, 기업에는 프로덕션 환경에서 거래 애플리케이션과 포트폴리오 관리 애플리케이션이 있으며, 두 애플리케이션 모두 투자 IT 팀에서 관리하며 많은 트래픽을 서로 교환합니다. 이 시나리오에서는 투자 IT 팀이 여러 애플리케이션 계정에 대한 액세스를 요청할 필요가 없고 회사가 트래픽 비용을 절감할 것이므로 회사가 동일한 계정과 동일한 VPC에서 두 애플리케이션을 그룹화하여 이점을 얻을 수 있습니다. 이 경우 회사는 개발 단계에서 동일한 애플리케이션에 대한 다른 계정을 생성하고 개발 팀에 액세스 권한을 제공해야 합니다.

또 다른 시나리오에서 기업은 인사 IT 팀과 회계 IT 팀에서 각각 관리하는 급여 애플리케이션과 회계 애플리케이션을 프로덕션 환경에 두고 있습니다. 급여 애플리케이션이 회계 애플리케이션과 정보를 교환해야 하지만 팀당 하나씩 서로 다른 계정에서 두 애플리케이션을 분리하고 네트워킹 계정을 사용하여 두 애플리케이션의 VPCs 간에 연결을 설정하는 것이 좋습니다. 이러한 방식으로 회사는 회계 애플리케이션 인프라에 영향을 미치는 HR IT 팀 요청 변경을 방지하며, 이 인프라에 대한 지식이 없습니다.

계정을 조직 단위(OU). OU는 계정을 분류(그룹화)하고 해당 그룹을 기반으로 정책 및 구성에 적용할 수 있는 논리적 그룹화 메커니즘입니다. OUs를 생성하는 데 권장되는 접근 방식은 보고 구조

내의 팀 내부 계층 구조가 아닌 특정 계정 그룹에 적용해야 하는 정책을 기반으로 하는 것입니다. OU는 Active Directory의 OU와 동일하지 않으며에서 AD OU 구조를 복제하려고 시도하는 AWS Organizations 것은 권장되지 않으므로 유지 관리 및/또는 운영 구조가 어렵습니다.

AWS 계정 제한

AWS 계정 한도는 AWS Managed Services(AMS) 계정에 적용됩니다. AWS 서비스의 기본 및 현재 제한을 결정하는 가장 쉬운 방법은 [AWS Service Quotas](#)를 활용하는 것입니다. AMS는 개별 서비스 제한을 적절한 크기로 조정하여 계정에서 서비스(들)를 실행할 것을 권장합니다. 제한은 보안 및 비용 런어웨이를 위해 계정을 보호하는 가드레일 역할을 합니다. 특정 한도를 높이려면 AMS에 서비스 요청을 제출하면 AMS Operations가 사용자를 대신하여 한도를 높입니다. 예를 들어 RDS 인스턴스의 기본 제한(또는 할당량)은 40입니다. 워크로드에 50개의 RDS 인스턴스가 필요한 경우 AMS 작업에 대한 서비스 요청을 제기하여 제한을 필요한 값으로 높입니다.

AMS 서비스 수준 목표(SLOs)

다음 표에서는 AWS Managed Services(AMS) 서비스의 목표를 설명합니다. 인시던트 관리를 포함하여 AMS 서비스의 다른 측면에 대한 서비스 수준 계약(SLAs)은 AMS를 구독할 때 공유되는 SLA 문서에서 다룹니다. 자세한 내용은 CSDM에 문의하세요.

AMS 서비스 수준 목표

Feature	성능 지표(PI)	더하기 (Business Days, M-F 8AM to 6PM local time)	프리미엄 (Calendar Days, 24 x 7)
변경 관리	자동 RFCs 예약하거나 거부하는 데 걸리는 시간	<=30분	<=30분
	예약된 실행 시간과 비교하여 예약된 RFCs 시작한 시간	<=1분	<=1분
	CT 카탈로그에서 사용할 수 있는 비자동 RFCs를 승인/거부하는 데 걸리는 시간	<=48시간	<=24시간

Feature	성능 지표(PI)	더하기 (Business Days, M-F 8AM to 6PM local time)	프리미엄 (Calendar Days, 24 x 7)
	CT 카탈로그에서 사용할 수 없는 자동화되지 않은 RFCs 승인/거부하는 데 걸리는 시간	<=5일	<=5일
문제 관리	근본 원인 분석(RCA)을 완료하는 데 걸린 시간	<=10일	<=10일
서비스 요청 관리	첫 번째 및 모든 후속 응답의 응답 시간	<=8시간	<=4시간

지원되는 AWS 서비스

AWS Managed Services(AMS)는 다음 서비스에 대한 운영 관리 지원 AWS 서비스를 제공합니다. 각 AWS 서비스는 고유하므로 AMS의 운영 관리 수준에 따라 기본 AWS 서비스의 특성과 특성에 따라 지원이 달라집니다. 특정 AWS 서비스는 AMS에서 제공하는 운영 관리 지원 서비스의 복잡성과 범위에 따라 그룹화됩니다.

Note

A, B, C의 세 그룹은 2021년 3월 16일 이전의 AMS 고객에 대한 지원 플랜(Plus 또는 Premium)을 기반으로 AMS 서비스에 대한 계정당 총 월별 지출의 백분율로 요금을 나타냅니다. 2021년 3월 16일 이후에 온보딩된 AMS 고객은 추가 요금 정보에 대한 서비스 요청을 제출해야 합니다. 그룹 A는 추가 요금이 없음을 나타냅니다. 그룹 B는 12%(Plus) 또는 18%(Premium)의 추가 요금을 나타냅니다. 그룹 C는 25%(Plus) 또는 42%(Premium)의 추가 요금을 나타냅니다. 별표(*) 1개는 고객이 AWS 콘솔 및 APIs를 사용하여 AMS 관리형 환경 내에 배포한 서비스를 나타냅니다. 이러한 방식으로 서비스를 프로비저닝하고 구성할 때 고객 책임에 대한 [AWS Managed Services\(AMS\) AMS Advanced 운영 계획 기능](#) 자세한 내용은의 '자동 및 셀프 서비스 프로비저닝 관리'를 참조하세요.

별 2개(**) AWS Outposts 는의 Amazon EC2가 그룹 B 서비스로 청구됨을 나타내며,에서 호스팅되는 다른 모든 리소스 AWS Outposts 는 표준 요금으로 청구됩니다.

지원되는 AWS 서비스

그룹 A	그룹 B	그룹 C
Amazon Alexa for Business* Amazon Managed Streaming for Apache Kafka* Amazon CloudFront Amazon Elastic File System Amazon Glacier Amazon Simple Storage Service AWS Amplify* AWS AppMesh* AWS Auto Scaling AWS Backup AWS CloudFormation AWS Compute Optimizer AWS Global Accelerator* AWS Identity and Access Management AWS License Manager* AWS Management Console AWS Marketplace AWS Lake Formation* AWS Well Architected Tool* VM Import/ Export*	Amazon API Gateway* Amazon AppStream* Amazon Athena* Amazon Bedrock* Amazon CloudSearch* Amazon Cognito* Amazon Comprehend* Amazon Connect* Amazon Document DB (with MongoDB compatibility)* Amazon DynamoDB* Amazon EC2 Container Registry (ECR)* Amazon Elastic Container Service (ECS) on AWS Fargate* Amazon Elastic Kubernetes Service (EKS) on Fargate* Amazon Elemental MediaConvert* Amazon Elemental MediaPackage* Amazon Elemental MediaStore* Amazon Elemental MediaTailor* Amazon Elastic MapReduce* AmazonEventBridge* Amazon Forecast* Amazon FSx* Amazon Inspector* Amazon Kendra* Amazon Kinesis Analytics* Amazon Kinesis Data Stream*	Amazon Aurora Amazon CloudWatch Amazon Elastic Block Store (EBS) Amazon Elastic Compute Cloud** Amazon Elastic Load Balancing (classic, application, and network; not gateway) Amazon ElastiCache Amazon OpenSearch Service Amazon GuardDuty Amazon Macie Amazon Redshift Amazon Relational Database Service Amazon Route 53 Amazon Route 53 Resolver DNS Firewall Amazon Simple Email Service Amazon Simple Notification Service Amazon Simple Queue Service Amazon Virtual Private Cloud (VPC) AWS CloudTrail AWS Config AWS Database Migration Service AWS Data Transfer AWS Direct Connect AWS Directory Service AWS Key Management Service

그룹 A	그룹 B	그룹 C
	Amazon Kinesis Firehose* Amazon Kinesis Video Streams* Amazon Lex* Amazon Managed Service for Prometheus* Amazon MQ* Amazon Personalize** Amazon Quantum Ledger Database (QLDB)* Amazon QuickSight* Amazon Rekognition* Amazon SageMaker* Amazon SimpleDB* Amazon Simple Workflow* Amazon Textract* Amazon Transcribe* Amazon Translate* Amazon WorkSpaces* AWS AppSync* AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM* AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS MigrationHub* AWS Outposts** AWS Resilience Hub* AWS Secrets Manager* AWS Security Hub* AWS Service Catalog	AWS Systems Manager (SSM)

그룹 A	그룹 B	그룹 C
	AWS Service Catalog AppRegistry* AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions* AWS Transit Gateway* AWS WAF* AWS X-Ray*	

아래에 명시적으로 지원되지 않는 소프트웨어 또는 서비스에 대한 서비스를 제공하도록 AWS Managed Services에 요청하는 경우 이러한 고객 요청 구성에 대해 제공되는 모든 AWS Managed Services는 서비스 약관에 따라 "베타 서비스"로 취급됩니다.

지원되는 구성

AWS Managed Services(AMS)에서 지원하는 구성은 다음과 같습니다.

- 언어: AMS는 영어로 제공됩니다.
- 방화벽 서비스:
 - Amazon Route 53 Resolver DNS 방화벽
 - Palo Alto VM 시리즈 차세대 방화벽
- 보안 소프트웨어: Trend Micro의 Deep Security(필수). AWS Marketplace: [Trend Micro Deep Security](#)
- 승인된 디렉터리 서비스: Microsoft Active Directory(AD)
- [지원되는 AWS 서비스](#).
- 지원되는 AWS 리전:

AMS는 모든 AWS 리전의 하위 집합에서 작동하지만 AMS API/CLI는 "미국 동부(버지니아 북부)" 리전에서만 실행됩니다. AMS 변경 관리 API(amscm) 또는 AMS 서비스 지식 관리 API(amsskms) 미국 이외의 동부 리전에서는 명령 `--region us-east-1`에 추가해야 합니다.

- 미국 동부(버지니아)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오리건)

- 미국 동부(오하이오)
- 캐나다(중부)
- 남아메리카(상파울루)
- EU(아일랜드)
- EU(프랑크푸르트)
- EU(런던)
- EU 서부(파리)
- 아시아 태평양(뭄바이)
- 아시아 태평양(서울)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(도쿄)
- Amazon 머신 이미지(AMIs): AMS는 AMS에서 지원하는 운영 체제 하위 집합에 대해 CIS 레벨 1 벤치마크를 기반으로 보안 강화 이미지(AMIs)를 제공합니다. 보안 강화 이미지를 사용할 수 있는 운영 체제를 찾으려면 AMS 보안 사용 설명서를 참조하세요. 이 가이드에 액세스하려면에서 AWS Managed Services에 대한 보고서 탭을 AWS Artifact필터링합니다. 에 액세스하려면 CSDM에 AWS Artifact문의하거나 [AWS 아티팩트 시작하기를](#) 참조하세요.
- 지원되는 운영 체제:

지원되는 운영 체제(x86-64)

- Amazon Linux 2023
- Amazon Linux 2(예상 AMS 지원 종료일 2026년 6월 30일)
- Oracle Linux 9.x, 8.x
- Red Hat Enterprise Linux(RHEL) 9.x, 8.x
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server for SAP 15 SP3 이상
- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

지원되는 운영 체제(ARM64)

- Amazon Linux 2023

- 지원되는 지원 종료(EOS) 운영 체제:

 Note

지원 종료(EOS) 운영 체제는 운영 체제 제조업체의 일반 지원 기간을 벗어나며 보안 위험이 증가합니다. EOS 운영 체제는 AMS 필수 에이전트가 운영 체제를 지원하는 경우에만 지원되는 구성으로 간주됩니다.

1. 업데이트를 받을 수 있도록 운영 체제 공급업체의 지원을 확대한 경우
 2. EOS 운영 체제를 사용하는 모든 인스턴스는 고급 사용 설명서의 AMS에서 지정한 [보안 제어](#)를 따르거나
 3. 사용자는 AMS에 필요한 기타 보상 보안 제어를 준수합니다.
- AMS가 더 이상 EOS 운영 체제를 지원할 수 없는 경우 AMS는 운영 체제를 업그레이드하기 위한 [중요 권장 사항을](#) 발행합니다.

AMS 필수 에이전트에는 Amazon CloudWatch AWS Systems Manager, 엔드포인트 보안 (EPS) 에이전트 및 Active Directory(AD) 브리지(Linux만 해당)가 포함될 수 있지만 이에 국한되지는 않습니다.

- Ubuntu Linux 18.04
- SUSE Linux Enterprise Server 15 SP3, SP4 및 SP5
- SUSE Linux Enterprise Server for SAP 15 SP2
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Service for SAP 12 SP5
- Microsoft Windows Server 2012/2012 R2
- Red Hat Enterprise Linux(RHEL):7.x
- Oracle Linux 7.5-7.9

AMS에서 지원되지 않는 운영 체제의 기능

지원되지 않는 운영 체제에는 나열되지 않은 운영 체제입니다. [지원되는 구성](#). AMS는 지원되지 않는 운영 체제가 있는 인스턴스를 [AWS 베타 및 미리 보기 서비스 약관이 적용되는 "고객 요청 구성"으로 간주합니다](#).

지원되지 않는 운영 체제가 있는 인스턴스에서는 다음과 같은 제한된 AMS 기능 세트를 사용할 수 있습니다.

기능	참고
인시던트 관리	AMS는 인시던트 대응을 제공합니다.
서비스 요청 관리	AMS는 서비스 요청에 응답합니다.
변경 요청(RFCs)	AMS는 실행을 위해 RFCs 평가합니다. 지원되지 않는 운영 체제는 RFCs.
모니터링	AMS는 Amazon EC2 시스템 상태 확인 및 인스턴스 상태 확인을 모니터링하고 이에 응답합니다. 시스템 상태 확인에는 네트워크 연결 손실, 시스템 전원 손실, 물리적 호스트의 소프트웨어 문제, 네트워크 연결성에 영향을 미치는 물리적 호스트의 하드웨어 문제가 포함됩니다. 인스턴스 상태 확인에는 잘못된 네트워킹 또는 시작 구성, 메모리 소진, 손상된 파일 시스템 및 호환되지 않는 커널이 포함됩니다.
보안 관리	AMS는 Amazon EC2 GuardDuty 조사 결과를 모니터링하고 이에 응답합니다.
백업 관리	AMS는 AMS 사용자 지정 계획 및 볼트를 사용하여 EC2 용 AMS Advanced에서 연속성 관리를 제공합니다. EC2 AWS Backup

AMS 고급 인터페이스

- AMS Advanced 콘솔: AMS Advanced 콘솔을 사용하여 RFCs를 생성하고, 인시던트를 보고 및 대응하고, 서비스 요청을 하고, 기존 VPCs 및 스택에 대한 정보를 찾을 수 있습니다. 어떻게 해야 할지 잘 모르겠거나 AMS 또는 관리형 리소스에 도움이 필요한 경우 인터페이스를 사용하여 서비스 요청을 생성합니다.
- AWS Management Console: 다음과 같이 많은 AWS 콘솔이 AMS 정보를 보는 데 유용할 수 있습니다.
 - Amazon EC2 콘솔: 접속 IP 주소, Amazon EC2 Auto Scaling 그룹 및 로드 밸런서를 포함한 인스턴스 정보를 보는 데 사용합니다.

- 다중 계정 랜딩 존 AWS Config 규칙 규정 준수: 계정 전체에서 규정 준수 상태를 보고 규정 미준수 리소스를 식별할 수 있습니다.
- AWS CloudFormation 콘솔: 스택 IDs 포함한 스택 정보를 보는 데 사용합니다(여기에서 Amazon RDS 스택 및 Amazon RDS 인스턴스 IDs와 이벤트 정보를 찾을 수 있음).
- Amazon RDS 콘솔: 계정의 사이트에서 WordPress 앱에 대한 게시물과 같은 이벤트 정보를 보는 데 사용합니다. Amazon RDS 인스턴스 ID가 있어야 합니다.

로그인 역할의 모드에 따라 AWS Management Console에 대한 액세스 수준이 다릅니다. 모드에 대한 자세한 내용은 [AMS 모드를](#) 참조하세요.

- AMS 고급 변경 관리 API - 읽기/쓰기: 변경 관리 API(CM API)를 사용하여 리소스 모니터링, 로그, 백업 및 패치 구성을 포함하여 관리형 인프라에 대한 추가 및 특정 변경을 요청합니다. 또한 이 API를 사용하여 리소스에 대한 액세스를 요청하고, 리소스를 삭제하고, AMIs 생성하고, IAM 인스턴스 프로파일을 생성합니다. AMS CLI 및 SDKs.
- AMS SKMS API - 읽기 전용: 이 API를 사용하여 관리형 리소스를 나열하고 변경 요청을 보고하거나 준비하는 데 필요한 정보를 가져옵니다.
- 지원 API: 표준 지원 API를 사용하여 인스턴트 및 서비스 요청을 프로그래밍 방식으로 생성하고 응답합니다. 자세한 내용은 [시작하기를 참조하세요 지원](#).
- AWS APIs- 읽기 전용: 기본 IT 관리자는 AWS APIs를 사용하여 관리 중인 모든 리소스를 보고, CloudTrail 로그, 결제 정보 및 기타 여러 읽기 함수를 볼 수 있습니다.

AMS VPC 엔드포인트

VPC 엔드포인트를 사용하면 인터넷 게이트웨이 AWS 서비스 없이도 VPC에 비공개로 연결할 수 있습니다. VPC의 인스턴스는 서비스의 리소스와 통신하는 데 퍼블릭 IP 주소를 필요로 하지 않습니다.

엔드포인트는 가상 디바이스입니다. 수평 확장되고 가용성이 높은 중복 VPC 구성 요소로, 가용성 위험이나 네트워크 트래픽에 대한 대역폭 제약 없이 VPC의 인스턴스와 서비스 간에 통신할 수 있도록 합니다. 자세한 내용은 [VPC 엔드포인트를 참조하세요](#).

VPC 엔드포인트에는 인터페이스 엔드포인트와 게이트웨이 엔드포인트라는 두 가지 종류가 있습니다.

- 게이트웨이 엔드포인트: 계정의 VPC에는 기본적으로 Amazon S3 Gateway 엔드포인트가 활성화되어 있습니다.
- 인터페이스 엔드포인트: AMS 환경의 인스턴스는 Amazon 네트워크를 벗어나지 않고도 지원되는 서비스와 통신할 수 있습니다. 이는 단일 계정 랜딩 존의 경우 선택 사항이며 계정에서 기본적으로 활

성화되지 않습니다. 이를 활성화하려면 AMS 작업에 서비스 요청을 제출하세요. 그러나 다중 계정 랜딩 존의 경우 공유 서비스 계정에서 인터페이스 엔드포인트가 기본적으로 활성화됩니다.

AMS에서 지원하는 인터페이스 엔드포인트 목록:

- AWS CloudFormation
- AWS CloudTrail
- AWS Config
- Amazon EC2 API
- AWS Key Management Service
- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- AWS Secrets Manager
- Amazon SNS
- AWS Systems Manager
- AWS Security Token Service

AMS 보호 네임스페이스

AWS Managed Services(AMS)의 보호된 네임스페이스 목록입니다. AWS 리소스를 사용할 때 이러한 네임스페이스를 사용하지 않음으로써 AMS와의 충돌을 방지합니다. 다른 AWS 서비스 네임스페이스에 대한 자세한 내용은 [Amazon 리소스 이름\(ARNs\) 및 AWS 서비스 네임스페이스를 참조하세요](#).

- `ams-*` (이는 새 리소스에 대해 선호되는 이름 지정 표준입니다.)
- `/ams/*` (경로 기반 리소스의 기본 이름 지정 표준)
- `AWSManagedServices*` (CamelCase가 적절한 리소스에 대해 선호되는 이름 지정 표준입니다.)
- `ams*` 및 `AMS*` 및 `Ams*`
- `AWS_*` 및 `aws*`
- `*/aws_reserved/*`
- `CloudTrail*` 및 `Cloudtrail*`
- `codedeploy_service_role`
- `customer-mc-*`
- `eps` 및 `EPS`

- EPSPMarketplaceSubscriptionRole
- EPSDB*
- IAMPolicy*
- INGEST*
- LandingZone*
- Managed_Services*
- managementhost
- mc* 및 MC* 및 Mc*
- MMS*
- ms-
- NewAMS*
- Root*
- sentinel* 및 Sentinel*
- sentinel.int.
- StateMachine*
- StackSet-ams*
- StackSet-AWS-Landing-Zone
- TemplateId*
- UnhealthyInServiceBastion
- VPC_*

AMS 예약 접두사

AMS 리소스 속성은 특정 패턴을 준수해야 합니다. 예를 들어 IAM 인스턴스 프로파일 이름, BackupVault 이름, 태그 이름 등은 AMS 예약 접두사로 시작해서는 안 됩니다. 이러한 예약 접두사는 다음과 같습니다.

```
*/aws_reserved/*  
ams - *  
/ams/*  
ams*  
AMS*  
Ams*
```

```
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion
```

AMS 유지 관리 기간

AWS Managed Services 유지 관리 기간(또는 유지 관리 기간)은 AWS Managed Services(AMS)에 대한 유지 관리 활동을 수행하고 태평양 표준시 기준 매월 두 번째 목요일 오후 3시부터 오후 4시까지 반복됩니다. AMS는 48시간 전에 통지하여 유지 관리 기간을 변경할 수 있습니다. 이는 AWS Managed Services(AMS)를 위한 것으로, 새 AMS AMIs.

유지 관리 기간은 AMS가 패치를 적용하고 온보딩 시 유지 관리 기간을 결정하는 시점입니다. 패치 서비스 알림에 제공된 제안된 패치 적용 기간에 동의하거나 다른 기간을 제안할 수도 있습니다.

유지 관리 기간 생성에 대한 지침은 [유지 관리 기간](#)을 참조하세요.

AMS 정보 리소스

AMS는 성공하는 데 도움이 되는 여러 정보 리소스를 제공합니다.

- AMS Accelerate 사용 설명서: AMS Accelerate가 제공하는 구성 요소 및 기능과 사용 방법을 이해하는 데 도움이 됩니다. 여기에서 AMS Accelerate 배경 정보 및 기본 설정, 조사 결과 리소스 및 방법 예제에 대한 세부 정보를 확인하세요. [HTML 인덱스](#), [PDF](#)
- AMS Advanced 사용 설명서: AMS Advanced가 제공하는 구성 요소 및 기능과 이를 사용하는 방법을 이해하는 데 도움이 됩니다. 여기에서 AMS 고급 배경 정보 및 기본 설정, 조사 결과 리소스 및 방법 예제에 대한 세부 정보를 확인하세요. [HTML 인덱스](#), [PDF](#)
- AMS Advanced Application Guide: 애플리케이션을 AWS Managed Services 인프라에 배포하는 단계를 설명합니다. 애플리케이션 배포 및 유지 관리 방법론과 고려 사항에 대한 자세한 내용은 여기를 참조하세요. [HTML 인덱스](#), [PDF](#).
- AMS 고급 온보딩 가이드: AMS 계정에서 기본 AWS Managed Services 다중 계정 또는 단일 계정 랜딩 존 인프라를 생성하는 초기 단계를 설명합니다. AMS 온보딩을 준비하기 위한 AMS 계정 기본 사항, 검증 및 질문에 대한 자세한 내용은 여기를 참조하세요. [HTML 인덱스](#), [PDF](#).
- AMS 고급 변경 유형 참조: 변경 유형 스키마와 각 변경 유형 및 팁에 대한 예제 연습을 포함하여 AWS Managed Services 제공하는 현재 변경 유형에 대한 참조 자료를 제공합니다. 변경 유형에 대한 일반 정보를 포함합니다. 변경 요청(RFCs) 및 AMS 변경 유형(CTs. 관련 정보에 대한 링크를 포함하여 변경 유형에 대한 세부 정보를 보려면 여기를 참조하세요. [HTML 인덱스](#), [PDF](#).
- AMS CM(변경 관리) API 참조: 변경 요청을 생성 및 모니터링하는 작업을 제공하고 AWS Managed Services 관리형 서비스 CM API를 설명합니다. [HTML 인덱스](#).
- AMS 보안 가이드: 독점 AMS 보안 정보를 설명합니다.

프라이빗, AWS Artifact 콘솔의 AMS 보고서 탭에서 사용할 수 있습니다.

- AMS 개발자의 리소스: amscm 및 amsskms 모두에 대해 AMS CLI 및 SDK에 액세스할 수 있습니다. <https://console.aws.amazon.com/managedservices/> 참조하십시오.
- AMS YouTube 동영상: 동영상에 설명된 주요 고객 작업입니다. [AWS Managed Services YouTube 지침 비디오를 참조하세요](#).
- AMS 블로그 게시물: AWS Managed Services에 대한 전문 정보입니다. [AWS 블로그를 참조하세요](#).

AMS 규정 준수

AMS는 다음 표준에 대한 감사를 거쳤으며 규정 준수 인증을 받아야 하는 솔루션의 일부로 사용할 수 있습니다.

AMS 지원 규정 준수 표준

AMS는 AWS 규정 준수 표준을 지원합니다. AWS 규정 준수 프로그램에 대한 자세한 내용은 [AWS 규정 준수를](#) 참조하세요.

다음은 AMS에서 지원하는 현재 규정 준수 표준입니다.

FedRAMP: 미국 연방 정부는 가장 혁신적이고 안전하며 비용 효율적인 방식으로 미국 사람들에게 서비스를 제공하는 데 전념합니다. 클라우드 컴퓨팅은 연방 정부가 운영 효율성을 달성하고 온디맨드로 혁신하여 국가 전체에서 미션을 발전시킬 수 있는 방법에 중요한 역할을 합니다. 이것이 오늘날 많은 연방 기관이 AWS 클라우드 서비스를 사용하여 연방 정부 데이터를 처리, 저장 및 전송하는 이유입니다.

자세한 내용은 [FedRAMP](#) 단원을 참조하세요.

HIPAA: AWS는 AMS를 HIPAA [적격 서비스로](#) 포함하도록 HIPAA(Health Insurance Portability and Accountability Act) 규정 준수 프로그램을 확장했습니다. AWS와 BAA(Business Associate Agreement)를 체결한 경우 AMS를 사용하여 HIPAA 준수 애플리케이션을 구축할 수 있습니다.

AMS를 사용하여 상태 정보를 처리하고 저장하는 방법을 알아보려면 [HIPAA 중심 백서를](#) 참조하세요. 자세한 내용은 [HIPAA 규정 준수](#)를 참조하세요.

HITRUST: Health Information Trust Alliance Common Security Framework(HITRUST CSF)는 GDPR, ISO, NIST, PCI 및 HIPAA와 같은 국가 및 국제적으로 허용되는 표준 및 규정을 활용하여 포괄적인 기준 보안 및 개인 정보 보호 제어 세트를 생성합니다.

자세한 내용은 [HITRUST CSF](#)를 참조하세요.

ISO 27001: ISO/IEC 27001:2013은 ISO/IEC 27002 모범 사례 지침에 따라 보안 관리 모범 사례와 포괄적인 보안 제어를 지정하는 보안 관리 표준입니다. 이 인증의 기반은 AWS가 총체적이고 포괄적인 방식으로 보안을 영구적으로 관리하는 방법을 정의하는

정보 보안 관리 시스템(ISMS)의 개발 및 구현을 포함하는 엄격한 보안 프로그램의 개발 및 구현입니다.

자세한 내용은 [ISO/IEC 27001:2013](#)을 참조하세요.

ISO 27017: ISO/IEC 27017:2015는 클라우드 컴퓨팅의 정보 보안 측면에 대한 지침을 제공하며, ISO/IEC 27002 및 ISO/IEC 27001 표준의 지침을 보완하는 클라우드별 정보 보안 제어 구현을 권장합니다. 이 연습 코드는 클라우드 서비스 공급자에 특정한 추가 정보 보안 제어 구현 지침을 제공합니다.

자세한 내용은 [ISO/IEC 27017:2015 규정 준수를](#) 참조하세요.

ISO 27018: ISO/IEC 27018:2019는 클라우드에서 개인 데이터를 보호하는 데 중점을 둔 실무 코드입니다. ISO/IEC 정보 보안 표준 27002를 기반으로 하며 퍼블릭 클라우드 개인 식별 정보(PII)에 적용되는 ISO/IEC 27002 제어에 대한 구현 지침을 제공합니다. 또한 기존 ISO/IEC 27002 제어 세트에서 다루지 않는 퍼블릭 클라우드 PII 보호 요구 사항을 해결하기 위한 일련의 추가 제어 및 관련 지침을 제공합니다.

자세한 내용은 [ISO/IEC 27018:2019 규정 준수를](#) 참조하세요.

ISO 9001: ISO 9001:2015는 조직 내에서 효과적인 품질 관리를 달성하는 데 필요한 구조, 책임 및 절차를 문서화하고 검토하는 프로세스 지향적 접근 방식을 간략하게 설명합니다. 표준의 특정 섹션에는 다음과 같은 주제에 대한 정보가 포함되어 있습니다.

- 품질 매뉴얼 문서화, 문서 제어, 프로세스 상호 작용 결정 등 품질 관리 시스템의 요구 사항
- 관리 책임
- 인적 자원 및 조직의 작업 환경을 포함한 리소스 관리
- 설계부터 제공까지 단계를 포함한 서비스 개발
- 고객 만족도
- 내부 감사, 시정 및 예방 조치와 같은 활동을 통한 GxP 측정, 분석 및 개선

자세한 내용은 [ISO 9001:2015 규정 준수를](#) 참조하세요.

PCI: AMS는 서비스 공급자 레벨 1에서 결제 카드 산업(PCI) 데이터 보안 표준(DSS) 버전 3.2에 대한 규정 준수 증명을 제공합니다. AWS 제품 및 서비스를 사용하여 카드 소지자 데이터를 저장, 처리 또는 전송하는 고객은 자체 PCI DSS 규정 준수 인증을 관리할 때 AMS를 사용할 수 있습니다.

AWS PCI 규정 준수 패키지의 사본을 요청하는 방법 같은 PCI DSS 관련 추가 정보는 [PCI DSS 레벨 1](#)을 참조하십시오. 중요한 것은 PCI DSS 버전 3.2 표준과 일치하도록 AMS에서 세분화된 암호 정책을 구성해야 한다는 것입니다. 적용해야 하는 정책에 대한 자세한 내용은 [AWS Microsoft AD 디렉터리에 대한 PCI 규정 준수 활성화를 참조하세요](#).

SOC: AMS 시스템 및 조직 제어(SOC) 보고서는 AMS가 주요 규정 준수 제어 및 목표를 달성하는 방법을 보여주는 독립적인 타사 검사 보고서입니다. 이러한 보고서의 목적은 사용자와 감사자가 운영 및 규정 준수를 지원하기 위해 설정된 AMS 제어를 이해하는데 도움이 되는 것입니다. AMS SOC 보고서에는 세 가지 유형이 있습니다.

- AWS SOC 1 보고서 - [AWS 아티팩트를 사용하여 다운로드](#)
- AWS SOC 2: 보안, 가용성 및 기밀성 보고서 - [AWS 아티팩트를 사용하여 다운로드](#)
- [AWS SOC 3: 보안, 가용성 및 기밀성 보고서](#)

자세한 내용은 [SOC 규정 준수를](#) 참조하세요.

공동 책임

PCI 규정 준수를 포함한 보안은 [공동 책임입니다](#). AMS 규정 준수 상태는 AWS 클라우드에서 실행하는 애플리케이션에 자동으로 적용되지 않는다는 점을 이해하는 것이 중요합니다. AWS 서비스 사용이 표준을 준수하는지 확인해야 합니다. AMS가 특정 활동에서 고객과 함께 작동하는 방식에 대한 자세한 내용은 AMS를 참조하세요 [AMS 책임 매트릭스\(RACI\)](#).

AMS Amazon Machine Image(AMIs)

AMS는 AMS 지원 운영 체제에 대해 매달 업데이트된 Amazon Machine Image(AMIs) 생성합니다. 또한 AMS는 AMIs)도 생성합니다. <https://docs.aws.amazon.com/managedservices/latest/userguide/supported-configs.html> 사용 가능한 보안 강화 이미지가 있는 운영 체제를 확인하려면 AWS Managed Services에 대해 필터링된 AWS Artifact -> 보고서 페이지(왼쪽 탐색 창에서 보고서 옵션 찾기)를 통해 사용할 수 있는 AMS 보안 사용 설명서를 참조하세요. AWS 아티팩트에 액세스하려면에서 CSDM에 문의하여 지침을 받거나 [AWS 아티팩트 시작하기로](#) 이동할 수 있습니다.

새 AMS AMIs 릴리스될 때 알림을 받으려면 "AMS AMI"라는 Amazon Simple Notification Service(Amazon SNS) 알림 주제를 구독하면 됩니다. 자세한 내용은 [SNS를 사용한 AMS AMI 알림을](#) 참조하세요.

AMS AMI 이름 지정 규칙은 `customer-ams-<operating system>-<release date> -<version>`(예: `customer-ams-rhel6-2018.11-3`).

로 시작하는 AMS AMIs만 사용합니다customer.

AMS는 항상 최신 AMI를 사용할 것을 권장합니다. 다음 중 하나를 통해 최신 AMIs

- AMS 콘솔의 AMIs 페이지를 살펴봅니다.
- CSDM에서 또는이 ZIP 파일을 통해 사용할 수 있는 최신 AMS AMI CSV 파일 보기: [ZIP의 AMS 11.2024 AMI 콘텐츠 및 CSV 파일](#).

과거 AMI ZIP 파일은 [문서 기록](#)을 참조하세요.

- 이 AMS SKMS 명령 실행(AMS SKMS SDK 필요):

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId,CreationTime]" --output table
```

운영 체제(OS)별로 AWS AMIs 콘텐츠

- Linux AMIs
 - [AWS CLI 도구](#)
 - [NTP](#)
 - [Trend Micro 엔드포인트 보호 서비스 에이전트](#)
 - [코드 배포](#)
 - [PBIS/신뢰할 수 없는 AD 브리지](#)
 - [SSM 에이전트](#)
 - 중요 패치에 대한 Yum 업그레이드
 - AMS 사용자 지정 스크립트/관리 소프트웨어(부트, AD 조인, 모니터링, 보안 및 로깅 제어)
- Windows Server AMIs
 - [Microsoft .NET Framework 4.5](#)
 - [PowerShell 5.1](#)
 - [AWS Windows PowerShell용 도구](#)
 - 부팅, AD 조인, 모니터링, 보안 및 로깅을 제어하는 AMS PowerShell 모듈
 - [Trend Micro 엔드포인트 보호 서비스 에이전트](#)
 - [SSM 에이전트](#)
 - [CloudWatch 에이전트](#)
 - EC2Config 서비스(Windows Server 2012 R2를 통해 제공)

- EC2Launch(Windows Server 2016 및 Windows Server 2019)
- EC2LaunchV2(Windows Server 2022 이상)

Linux 기반 AMIs

- Amazon Linux 2023(최신 마이너 릴리스)(최소 AMI는 지원되지 않음)
- Amazon Linux 2(최신 마이너 릴리스)
- Amazon Linux 2(ARM64)
- Red Hat Enterprise 7(최신 마이너 릴리스)
- Red Hat Enterprise 8(최신 마이너 릴리스)
- Red Hat Enterprise 9(최신 마이너 릴리스)
- SUSE Linux Enterprise Server 15 SP6
- Ubuntu Linux 18.04
- Ubuntu Linux 20.04
- Ubuntu Linux 22.04
- Ubuntu Linux 24.04
- Amazon Linux: 제품 개요, 요금 정보, 사용 정보 및 지원 정보는 [Amazon Linux AMI\(HVM/64비트\)](#) 및 [Amazon Linux 2](#)를 참조하세요.

자세한 내용은 [Amazon Linux 2 FAQs](#)를 참조하세요.

- RedHat Enterprise Linux(RHEL): 제품 개요, 요금 정보, 사용 정보 및 지원 정보는 [Red Hat Enterprise Linux\(RHEL\) 7\(HVM\)](#)을 참조하세요.
- Ubuntu Linux 18.04: 제품 개요, 요금 정보, 사용 정보 및 지원 정보는 [Ubuntu 18.04 LTS - Bionic](#)을 참조하세요.
- SUSE Linux Enterprise Server for SAP 애플리케이션 15 SP6:
 - 계정당 다음 단계를 한 번 실행합니다.
 1. AWS Marketplace로 이동합니다.
 2. SUSE 15 SAP 제품을 검색합니다.
 3. 계속 구독하기(Continue to Subscribe)를 선택합니다.
 4. 약관에 동의를 선택합니다.
 - 새 SUSE Linux Enterprise Server for SAP Applications 15 SP6 인스턴스를 시작해야 할 때마다 다음 단계를 완료하세요.

1. 구독한 SUSE Linux Enterprise Server for SAP Applications 15 AMI의 AMI ID를 기록해 둡니다.
2. 배포 생성 | 고급 스택 구성 요소 | EC2 스택 | 변경 유형 생성 ct-14027q0sjyt1h RFC.
*InstanceAmiId*를 구독한 AWS Marketplace AMI ID로 바꿉니다.

Windows 기반 AMIs

최신 Windows AMIs를 기반으로 하는 Microsoft Windows Server(2016, 2019 및 2022).

AMIs. <https://docs.aws.amazon.com/managedservices/latest/ctref/ex-ami-create-col.html>

AMS AMIs 오프보딩:

AMS는 종속성에 영향을 주지 않도록 오프보딩 중에 AMIs를 공유 해제하지 않습니다. 계정에서 AMS AMIs 제거하려면 `cancel-image-launch-permission` API를 사용하여 특정 AMIs를 숨길 수 있습니다. 예를 들어 아래 스크립트를 사용하여 이전에 계정과 공유된 모든 AMS AMIs를 숨길 수 있습니다.

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
    aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

스크립트가 오류 없이 실행되려면 AWS CLI v2가 설치되어 있어야 합니다. AWS CLI 설치 단계는 [AWS CLI의 최신 버전 설치 또는 업데이트를 참조하세요](#). `cancel-image-launch-permission` 명령에 대한 자세한 내용은 섹션을 참조하세요 [cancel-image-launch-permission](#).

보안 강화 AMIs

AMS는 AMS가 지원하는 운영 체제의 하위 집합에 대해 CIS 레벨 1 벤치마크를 기반으로 보안 강화 이미지(AMIs)를 제공합니다. 사용 가능한 보안 강화 이미지가 있는 운영 체제를 찾으려면 AWS Managed Services(AMS) 고객 보안 가이드를 참조하세요. 이 가이드에 액세스하려면 왼쪽 탐색 창에서 보고서를 열고 AWS Artifact선택한 다음 AWS Managed Services를 필터링합니다. 에 액세스하는 방법에 대한 지침은 CSDM에 AWS Artifact문의하거나 [AWS Artifact](#) 시작하기에서 자세한 내용을 참조하세요.

AD FS와 AMS 간의 통합 작동 방식

온프레미스 네트워크와 AMS 도메인 간의 단방향 신뢰는 스택 및 VPCs. VPC 및 스택이 생성되면 미리 구성된 Active Directory 보안 그룹을 통해 액세스 권한이 부여됩니다. 또한 AWS 관리 콘솔에 대한

Single Sign-On(SSO)에 대해 Active Directory Federation Service(AD FS) 또는 SAML을 지원하는 모든 페더레이션 소프트웨어를 사용하여에 대한 액세스를 구성할 AWS Management Console 수 있습니다.

 Note

AMS는 여러 페더레이션 서비스, Ping, Okta 등에 페더레이션할 수 있습니다. AD FS로 제한되지 않습니다. 여기서는 사용 가능한 하나의 페더레이션 기술의 예를 제공합니다.

여기 정보는 [Windows Active Directory, AD FS 및 SAML 2.0을 AWS 사용하여에 페더레이션 활성화](#) 블로그 게시물에서 중복됩니다.

1. 사용자(Bob이라고 함)가 도메인 내의 AD FS 샘플 사이트(<https://Fully.Qualified.Domain.Name.Here/adfs/ls/IdpInitiatedSignOn.aspx>)를 탐색하면 흐름이 시작됩니다. AD FS를 설치하면이 페이지가 포함된 기본 웹 사이트의 adfs라는 새 가상 디렉터리가 나타납니다.
2. 로그인 페이지는 AD에 대해 Bob을 인증합니다. Bob이 사용 중인 브라우저에 따라 AD 사용자 이름과 암호를 입력하라는 메시지가 표시될 수 있습니다.
3. Bob의 브라우저는 AD FS로부터 인증 응답의 형태로 SAML 어설션을 수신합니다.
4. Bob의 브라우저는 SAML 어설션을 SAML AWS 의 로그인 엔드포인트(<https://signin.aws.amazon.com/saml>)에 게시합니다. 백그라운드에서 로그인은 [AssumeRoleWithSAML](#) API를 사용하여 임시 보안 자격 증명을 요청한 다음에 대한 로그인 URL을 구성합니다 AWS Management Console.
5. Bob의 브라우저는 로그인 URL을 수신하고 콘솔로 리디렉션됩니다.

Bob의 관점에서 볼 때 프로세스는 투명하게 이루어집니다. 그는 내부 웹 사이트에서 시작하여 자격 AWS 증명을 제공할 필요 AWS Management Console없이에서 끝납니다.

 Note

AMS 콘솔에 대한 페더레이션 구성에 대한 자세한 내용은 다음을 참조하십시오.

- 다중 계정 랜딩 존: [AMS 콘솔에 대한 페더레이션 구성](#)
- 단일 계정 랜딩 존: [AMS 콘솔에 대한 페더레이션 구성](#)

또한 [부록: AD FS 클레임 규칙 및 SAML 설정](#)을 참조하세요. AWS Microsoft AD를 사용하여 규정 준수 요구 사항이 적용되는 AWS 클라우드에서 Active Directory 인식 애플리케이션을 지원하는 방법에 대한 자세한 내용은 [Microsoft AD 규정 준수 관리](#)를 참조하세요.

AMS 관리형 Active Directory

AMS는 이제 AMS가 Active Directory(AD) 인프라 작업을 관리하는 동시에 Active Directory 관리를 제어할 수 있도록 하는 Managed Active Directory(Managed AD)라는 새로운 서비스를 제공합니다.

Managed AD에 대한 AMS 지원은 Amazon Relational Database Service(RDS)에 대한 AMS 지원과 유사합니다. 두 경우 모두 AWS (AMS 포함)는 액세스 제어 및 모든 관리 기능을 수행하는 동안 서비스를 실행하는 인프라의 생성 및 관리를 지원합니다. 이 모델의 장점은 다음과 같습니다.

- 보안 위험을 제한합니다. AWS 또한 AMS에는 도메인에 대한 관리 권한이 필요하지 않습니다.
- 직접 통합: AMS와 인터페이스할 필요 없이 현재 권한 부여 모델을 사용하고 AD와 통합할 수 있습니다.

참고:

- AMS와 사용자 모두 Managed AD 도메인 컨트롤러에 액세스할 수 없으므로 도메인 컨트롤러에 소프트웨어를 설치할 수 없습니다. 이는 도메인 컨트롤러에 소프트웨어를 설치해야 하는 타사 솔루션이 허용되지 않기 때문에 중요합니다.

액세스는 다음과 같이 작동합니다.

- AWS 디렉터리 서비스 팀: 도메인 컨트롤러에 액세스할 수 있습니다.
- AMS: 디렉터리 서비스 APIs에 액세스하여 도메인에서 특정 작업을 수행할 수 있습니다. 이러한 작업에는 AD 스냅샷 생성, AD 스키마 변경 및 기타 작업이 포함됩니다.
- 사용자: 사용자, 그룹 등을 생성하기 위해 도메인(AD)에 액세스할 수 있습니다.
- 기존 AD 환경의 모든 기능을 관리형 AD 환경에서 사용할 수 있는 것은 아니므로 기업 AD를 마이그레이션하기 전에 관리형 AD에 대한 개념 증명을 수행하는 것이 좋습니다.
- AMS는 AD 관리를 관리하거나 이에 대한 지침을 제공하지 않습니다. 예를 들어 AMS는 조직 단위 구조, 그룹 정책 구조, AD 사용자 이름 지정 규칙 등에 대한 지침을 제공하지 않습니다.

다음과 같이 작동합니다.

1. AMS는 AMS 계정과 AWS 계정 별개로 새를 온보딩하고 Directory Service를 통해 Active AWS Directory(AD) 환경을 프로비저닝합니다([AWS Directory Service란 무엇입니까?](#) 참조).

다음은 AMS가 Managed AD에 온보딩하기 위해 시스템 통합자가 사용자로부터 수집해야 하는 정보입니다.

- 계정 정보
 - AMS 관리형 AD: AWS 계정 number에 대해 AWS 계정 생성된의 계정 ID
 - Managed AD를 온보딩할 리전: AWS 리전
- 관리형 Active Directory 정보:
 - Microsoft AD Edition: Standard/Enterprise. AWS Microsoft AD(Standard Edition)에는 1GB의 디렉터리 객체 스토리지가 포함되어 있습니다. 이 용량은 최대 5,000명의 사용자 또는 사용자, 그룹, 컴퓨터를 포함한 30,000개의 디렉터리 객체를 지원할 수 있습니다. AWS Microsoft AD(Enterprise Edition)에는 최대 100,000명의 사용자 또는 500,000개의 객체를 지원할 수 있는 17GB의 디렉터리 객체 스토리지가 포함되어 있습니다.

자세한 내용은 [AWS Directory Service FAQs](#).

- 도메인 FQDN: AMS 관리형 AD 도메인의 FQDN입니다.
- 도메인 NetBIOS 이름: AMS 관리형 AD 도메인의 NetBIOS 이름입니다.
- Managed AD 통합을 원하는 AMS 표준 계정의 계정 번호(AMS는 AMS 표준 계정의 AD에서 Managed AD로의 단방향 신뢰 구성)
- Active Directory 스키마 수정이 필요하고 필요한 경우 어떤 수정이 필요합니까?
- 기본적으로 두 개의 도메인 컨트롤러가 프로비저닝됩니다. 더 필요합니까? 그렇다면 필요한 것은 몇 개이며 그 이유는 무엇입니까?
- 관리형 Active Directory에 대한 네트워킹 정보:
 - 도메인 컨트롤러용 관리형 AD VPC CIDR(관리형 AD 도메인 컨트롤러용 프라이빗 서브넷 범위의 CIDR):
 - 도메인 컨트롤러용 서브넷 CIDR 1: [CIDR, AMS 관리형 AD VPC CIDR의 일부여야 함]
 - 도메인 컨트롤러용 서브넷 CIDR 2: [CIDR, AMS 관리형 AD VPC CIDR의 일부여야 함]

예:

- 관리형 AD VPC CIDR: 192.168.0.0/16
- 도메인 컨트롤러의 CIDR 1: 192.168.1.0/24
- 도메인 컨트롤러의 CIDR 2: 192.168.2.0/24

IP 주소 충돌을 방지하려면 지정한 Managed AD VPC CIDR이 회사 네트워크에서 사용 중인 다른 프라이빗 서브넷 CIDR과 충돌하지 않도록 해야 합니다.

- VPN 기술(선택 사항): [Direct Connect/Direct Connect 및 VPN]
 - 게이트웨이의 BGP 자율 시스템 번호(ASN): [고객 제공 ASN]
 - 게이트웨이 외부 인터페이스의 인터넷 라우팅 가능 IP 주소입니다. 주소는 정적이어야 합니다. [고객 제공 IP 주소]
 - VPN 연결에 정적 경로가 필요한지 여부: [예/아니요]
2. AMS는 AD 환경에 대한 관리자 계정 암호를 제공하고 AMS 엔지니어가 더 이상 AD 환경에 액세스할 수 없도록 암호를 재설정하도록 요청합니다.
 3. 관리자 계정 암호를 재설정하려면 Active Directory 사용자 및 컴퓨터(ADUC)를 사용하여 Active Directory 환경에 연결합니다. ADUC 및 기타 원격 서버 관리 도구(RSAT)는 비 AMS 인프라에서 사용자가 프로비저닝한 관리 호스트에 설치하고 실행해야 합니다. Microsoft에는 이러한 관리 호스트를 보호하는 모범 사례가 있습니다. 자세한 내용은 [보안 관리 호스트 구현을 참조하세요](#). 이러한 관리 호스트를 사용하여 Active Directory 환경을 관리합니다.
 4. 일상적인 작업에서 AMS는 VPC 구성, AD 백업, AD 신뢰 생성 및 삭제 등과 같은 사물의 AWS 디렉터리 서비스 측 AWS 계정 까지를 관리합니다. 사용자 생성, 그룹 생성, 그룹 정책 생성 등과 같은 AD 환경을 사용하고 관리합니다.

최신 RACI 테이블은 [서비스 설명](#) 참조의 "역할 및 책임" 섹션을 참조하세요.

AMS 애플리케이션 배포

AMS 애플리케이션 개발자 안내서에서는 다음 배포에 대한 자세한 설명과 연습을 제공합니다.

- AMS 워크로드 수집 CT를 사용하면 사용자와 AMS 클라우드 마이그레이션 파트너가 기존 워크로드를 AMS 관리형 VPC로 쉽게 이동할 수 있습니다. AMS 워크로드 수집을 사용하면 배포 | 수집 | 마이그레이션 파트너의 스택 마이그레이션된 인스턴스 | CT 생성(ct-257p9zjk14ija)이 포함된 RFC를 제출하여 AMS AMI를 생성할 수 있습니다. 마이그레이션 AWS 파트너가 온프레미스에서 로 마이그레이션한 인스턴스와 인스턴스를 수집할 대상 AMS VPC 및 서브넷이 있어야 합니다.

자세한 내용은 [워크로드 수집](#)의 AMS 애플리케이션 개발자 안내서를 참조하세요.

- 변경 유형 AWS CloudFormation 수집(ct-36cn2avfrrj9v) 기능을 사용하면 기존 CloudFormation 템플릿을 사용하여 AMS 관리형 VPC에 사용자 지정 스택을 쉽게 배포할 수 있습니다.

자세한 내용은 [CloudFormation 템플릿 수집](#)의 AMS 애플리케이션 개발자 가이드를 참조하세요.

- 온프레미스 데이터베이스를 AMS 관리형 Amazon S3 버킷 또는 Amazon RDS 인스턴스로 새 데이터베이스로 가져올 수 있습니다. 이 작업은 복제 인스턴스 생성(ct-27aplkhqr0ol), 복제 서브넷 그룹 생성(ct-2q5azjd8p1ag5), 복제 작업 생성(ct-1d2fml15b9eth), 소스 엔드포인트 생성(ct-0attesnjy2cx) 또는 소스 엔드포인트 생성(S3)(ct-2oxl37nphsrjz) 및 대상 엔드포인트 생성(ct-3gf8dolbo8x9p) 또는 대상 엔드포인트 생성(S3)(ct-05muqzievnxk5)을 포함한 배포 | 고급 스택 구성 요소 | 데이터베이스 마이그레이션 서비스(DMS) 변경 유형을 사용하여 수행합니다.

자세한 내용은 [Database Migration Service](#)의 AMS 애플리케이션 개발자 안내서를 참조하세요.

- 온프레미스 MS SQL 데이터베이스를 AMS 관리형 RDS SQL 인스턴스의 새 데이터베이스로 가져올 수 있습니다. 다양한 AMS 변경 유형과 Amazon RDS API 및 AWS 콘솔을 사용하여이 작업을 수행할 수 있습니다.

자세한 내용은 [데이터베이스\(DB\)에서 MS SQL RDS로 가져오기](#)의 AMS 애플리케이션 안내서를 참조하세요.

AWS Managed Services의 서비스 관리

주제

- [AWS Managed Services의 계정 거버넌스](#)
- [AWS Managed Services에서 서비스 시작](#)
- [고객 관계 관리\(CRM\)](#)
- [AWS Managed Services의 비용 최적화](#)
- [AWS Managed Services의 서비스 시간](#)
- [AWS Managed Services에 대한 도움말 보기](#)

AMS 서비스가 작동하는 방식입니다.

AWS Managed Services의 계정 거버넌스

이 섹션에서는 AMS 계정 거버넌스를 다룹니다.

AMS 전반에 걸쳐 자문 지원을 제공하고 관리형 환경의 사용 사례 및 기술 아키텍처를 자세히 이해하는 클라우드 서비스 제공 관리자(CSDM)로 지정됩니다. CSDMs 계정 관리자, 기술 계정 관리자, AWS Managed Services 클라우드 아키텍트(CAs) 및 해당하는 경우 AWS 솔루션 아키텍트(SAs)와 협력하여 소프트웨어 개발 및 운영 프로세스 전반에 걸쳐 새 프로젝트를 시작하고 모범 사례 권장 사항을 제공하는 데 도움이 됩니다. CSDM은 AMS의 기본 연락 지점입니다. CSDM의 주요 책임은 다음과 같습니다.

- 고객과 월별 서비스 검토 회의를 조직하고 주도합니다.
- 보안, 환경의 소프트웨어 업데이트 및 최적화 기회에 대한 세부 정보를 제공합니다.
- AMS에 대한 기능 요청을 포함하여 요구 사항을 충족합니다.
- 결제 및 서비스 보고 요청에 대응하고 해결합니다.
- 재무 및 용량 최적화 권장 사항에 대한 인사이트를 제공합니다.

AWS Managed Services에서 서비스 시작

서비스 시작: AWS Managed Services 계정의 서비스 시작 날짜는 AWS가 해당 AWS Managed Services 계정의 온보딩 요구 사항에 명시된 활동이 완료되었음을 알리는 첫 번째 달의 첫 번째 날입니다.

다. 단, AWS가 해당 월의 20일 이후에 알림을 보내는 경우 서비스 시작 날짜는 해당 알림 날짜 다음 달의 두 번째 날입니다.

서비스 시작

- R은 작업을 수행하기 위해 작업을 수행하는 책임 당사자를 나타냅니다.
- 나는 종종 작업 또는 결과물 완료 시에만 진행 상황에 대한 정보를 받는 당사자인 정보를 의미합니다.

서비스 시작

단계 #	단계 제목	설명	Customer	AMS
1.	고객 AWS 계정 인계	고객이 새 AWS 계정을 생성하고 이를 AWS Managed Services로 인계합니다.	R	정보
2.	AWS Managed Services 계정 - 디자인	AWS Managed Services 계정의 설계 완료	정보	R
3.	AWS Managed Services 계정 - 빌드	AWS Managed Services 계정은 2단계의 설계에 따라 빌드됩니다.	정보	R

고객 관계 관리(CRM)

AWS Managed Services(AMS)는 고객 관계 관리(CRM) 프로세스를 제공하여 잘 정의된 관계가 설정되고 유지되도록 합니다. 이 관계의 기반은 비즈니스 요구 사항에 대한 AMS의 인사이트를 기반으로 합니다. CRM 프로세스를 통해 다음을 정확하고 포괄적으로 이해할 수 있습니다.

- 비즈니스 요구 사항 및 이러한 요구 사항을 충족하는 방법
- 기능 및 제약 조건
- AMS 및 다양한 책임과 의무

CRM 프로세스를 통해 AMS는 일관된 방법을 사용하여 서비스를 제공하고 AMS와의 관계에 대한 거버넌스를 제공할 수 있습니다. CRM 프로세스에는 다음이 포함됩니다.

- 주요 이해관계자 식별
- 거버넌스 팀 구성
- 나와 함께 서비스 검토 회의 수행 및 문서화
- 에스컬레이션 절차를 통해 공식 서비스 불만 제기 절차 제공
- 만족도 및 피드백 프로세스 구현 및 모니터링
- 계약 관리

CRM 프로세스

CRM 프로세스에는 다음과 같은 활동이 포함됩니다.

- 비즈니스 프로세스 및 요구 사항 식별 및 이해. AMS와의 계약은 이해관계자를 식별합니다.
- 요구 사항 및 요구 사항에 맞게 제공할 서비스를 정의합니다.
- 서비스 검토 회의에서 회의를 통해 AMS 서비스 범위, SLA, 계약 및 비즈니스 요구 사항의 변경 사항에 대해 논의합니다. 성과, 업적, 문제 및 실행 계획을 논의하기 위해 임시 회의를 개최할 수 있습니다.
- 고객 만족도 설문 조사와 회의에서 제공된 피드백을 사용하여 만족도를 모니터링합니다.
- 내부적으로 측정된 월별 성능 보고서에 대한 성능 보고.
- 서비스를 함께 검토하여 개선 기회를 결정합니다. 여기에는 제공된 AMS 서비스의 수준 및 품질과 관련하여 사용자와 자주 소통하는 것이 포함됩니다.

CRM 회의

AMS 클라우드 서비스 제공 관리자(CSDMs) 정기적으로 회의를 개최하여 서비스 트랙(운영, 보안 및 제품 혁신) 및 경영진 트랙(SLA 보고서, 만족도 측정 및 비즈니스 요구 사항 변경)에 대해 논의합니다.

회의	용도	Mode	Participants
주간 상태 검토 (선택 사항)	미해결 문제 또는 인시던트, 패치, 보안 이벤트, 문제 레코드 12주 운영 추세 +/- 6) 애플리케이션 운영자 문제	현장 고객 location/ Telecom/Chime	AMS: CSDM 및 클라우드 아키텍트(CA) 고객이 할당한 팀원(예: 클라우드/인프라, 애플리케이션)

회의	용도	Mode	Participants
	주말 일정		이션 지원, 아키텍처 팀 등)
월별 비즈니스 검토	서비스 수준 성능 검토(보고서, 분석 및 추세) 재무 분석 제품 로드맵 CSAT	현장 고객 location/ Telecom/Chime	AMS: CSDM, 클라우드 아키텍트 (CA), AMS 계정 팀, AMS 기술 제품 관리자(TPM)(선택 사항), AMS OPS 관리자(선택 사항) 사용자: Application Operator 담당자
분기별 비즈니스 검토	접수료 및 서비스 수준 계약(SLA) 성능 및 추세(6개월) 향후 3/6/9/12개월 계획/마이그레이션 위험 및 위험 완화 주요 개선 이니셔티브 제품 로드맵 항목 미래 방향 일치 기회 재무 비용 절감 이니셔티브 비즈니스 최적화	현장 고객 위치	AMS: CSDM, 클라우드 아키텍트, AMS 계정 팀, AMS 서비스 디렉터, AMS 운영 관리자 사용자: 애플리케이션 운영자 담당자, 서비스 담당자, 서비스 디렉터

CRM 회의 계약

AMS CSDM은 다음을 포함하여 회의를 문서화할 책임이 있습니다.

- 작업 항목, 문제 및 참석자 목록을 포함한 의제 생성.
- 각 회의에서 검토한 작업 항목 목록을 생성하여 항목이 일정에 따라 완료되고 해결되었는지 확인합니다.
- 회의 후 영업일 기준 1일 이내에 이메일로 회의록과 작업 항목 목록을 회의 참석자에게 배포합니다.
- 회의록을 적절한 문서 리포지토리에 저장합니다.

CSDM이 없는 경우 회의를 주도하는 AMS 담당자가 회의록을 생성하고 배포합니다.

Note

CSDM은 사용자와 협력하여 계정 거버넌스를 설정합니다.

CRM 월별 보고서

AMS CSDM은 월별 서비스 성능 프레젠테이션을 준비하고 전송합니다. 프레젠테이션에는 다음에 대한 정보가 포함되어 있습니다.

- 보고서 날짜
- 요약 및 인사이트:
 - 주요 콜 아웃: 총 및 활성 스택 수, 스택 패치 상태, 계정 온보딩 상태(온보딩만 해당), 고객별 문제 요약
 - 성능: 인시던트 해결, 알림, 패치 적용, 변경 요청(RFCs), 서비스 요청, 콘솔 및 API 가용성에 대한 통계
 - 문제, 과제, 우려 사항 및 위험: 고객별 문제 상태
 - 예정된 항목: 고객별 온보딩 또는 인시던트 해결 계획
- 관리형 리소스: 스택의 그래프 및 파이형 차트
- AMS 지표: 모니터링 및 이벤트 지표, 인시던트 지표, AMS SLA 준수 지표, 서비스 요청 지표, 변경 관리 지표, 스토리지 지표, 연속성 지표, Trusted Advisor 지표 및 비용 요약(여러 가지 방법 제시). 기능 요청. 연락처 정보.

Note

설명된 정보 외에도 CSDM은 운영 활동에 대한 AMS의 하청업체 사용을 포함하여 범위 또는 조건의 중요한 변경 사항을 알려줍니다.

AMS는 CSDM이 월별 보고서에 포함하는 패치 및 백업에 대한 보고서를 생성합니다. 보고서 생성 시스템의 일부로 AMS는 사용자가 액세스할 수 없는 일부 인프라를 계정에 추가합니다.

- 원시 데이터가 보고된 S3 버킷
- 데이터를 쿼리하기 위한 쿼리 정의가 있는 Athena 인스턴스
- S3 버킷에서 원시 데이터를 읽기 위한 Glue 크롤러

AWS Managed Services의 비용 최적화

AWS Managed Services는 월별 비즈니스 검토(MBRs) 중에 매월 상세한 비용 사용률 및 절감 보고서를 제공합니다.

AMS는 표준 프로세스 및 메커니즘 세트를 따라 관리형 계정의 비용 절감 방법을 식별하고 AWS 지출을 최적화하기 위해 변경 사항을 계획하고 롤아웃하는 데 도움이 됩니다.

Note

AMS는 비용 최적화에 도움이 되는 비디오를 개발하고 있습니다. 첫 번째 단계는 비용 최적화 모범 사례의 PDF 및 Excel 스프레드시트를 제공하는 것입니다. 이러한 리소스에 액세스하려면 [비용 최적화 ZIP 파일에 대한 빠른 안내서](#)를 엽니다.

비용 최적화 프레임워크

AMS는 AWS 비용을 최적화하기 위해 3단계 접근 방식을 따릅니다.

1. 관리형 환경에서 비용 최적화 방법 식별
2. 비용 최적화 계획을 제시하세요.
3. 측정 가능한 방식으로 비용 최적화 달성 지원

관리형 환경에서 비용 최적화 방법 식별

AMS는 Cost Explorer 및 Trusted Advisor와 같은 AWS 네이티브 도구를 활용하는 동시에 아키텍처 최적화, EC2 인스턴스 및 AWS 계정 중심 최적화 전반에서 20개 이상의 비용 절감 패턴을 활용하여 맞춤형 비용 절감 권장 사항을 구축합니다.

최적화 권장 사항 중 일부는 다음과 같습니다.

아키텍처 최적화 권장 사항:

- **최적의 S3 스토리지 클래스 사용:** Amazon S3는 데이터 액세스, 복원력 및 비용에 따라 다양한 워크로드 요구 사항을 충족하는 다양한 스토리지 클래스를 제공합니다. 워크로드 요구 사항에 따른 S3 Intelligent-Tiering 및 S3 스토리지 클래스 분석을 통해 S3 비용을 효율적으로 관리할 수 있습니다.
- **캐싱 아키텍처 사용:** 해당하는 경우 캐시 인스턴스를 활용하면 IOPS 요구 사항을 충족하면서 일부 데이터베이스 인스턴스를 교체할 수 있습니다.
- **EBS 업그레이드 비용 절감:** EBS 볼륨을 gp2에서 gp3로 마이그레이션하면 최대 20%의 비용을 절감할 수 있으며 볼륨 크기에 관계없이 예측 가능한 3,000IOPS 기준 성능과 125MiB/s를 활용할 수 있습니다.
- **탄력성 사용:** AWS 제공하는 Auto Scaling 기능을 사용하면 비용 최적화를 위한 효과적인 리소스 사용률과 방법을 얻을 수 있습니다. 필요에 따라 인스턴스 조정 정책을 정기적으로 검토하고 업데이트하면 비용을 절감할 수 있습니다.

EC2 인스턴스 중심 권장 사항

- **인스턴스 크기 조정:** 인스턴스 크기 조정 및 사용량에 따른 최적의 구성에 중점을 둔 권장 사항입니다. 권장 사항에는 Amazon EC2 Auto Scaling 기능 활용 및 해당하는 경우 EC2 인스턴스를 Amazon S3의 AWS Lambda 또는 정적 웹 콘텐츠 등으로 대체하는 것도 포함됩니다.
- **인스턴스 예약:** AMS Resource Scheduler를 사용하여 시간 일정에 따라 인스턴스를 자동으로 시작 및 중지하면 특히 업무 외 시간에 활용되지 않는 비프로덕션 인스턴스에 대한 비용을 절감하는 데 도움이 됩니다.
- **절감형 플랜 구독:** 절감형 플랜은 AWS 사용량을 절약하는 가장 쉬운 방법입니다. EC2 Instance Savings Plans은 Amazon EC2 인스턴스 사용량에 대한 온디맨드 요금에 비해 최대 72%의 절감 효과를 제공합니다. Amazon SageMaker AI Savings Plans은 Amazon SageMaker AI 서비스 사용량을 최대 64% 절감합니다. AMS는 AWS 리소스 사용량에 따라 절감형 플랜에 대한 적절한 권장 사항을 제공합니다.
- **예약 인스턴스(RI) 사용 및 소비 지침:** Amazon EC2 예약 인스턴스(RI)는 온디맨드 요금에 비해 상당한 할인(최대 75%)을 제공하고 특정 가용 영역에서 사용할 경우 용량 예약을 제공합니다.
- **스팟 인스턴스 사용:** 내결함성 워크로드는 스팟 인스턴스를 활용하고 가격을 최대 90%까지 줄일 수 있습니다.
- **유휴 인스턴스 종료:** 유휴 상태이거나 종료할 수 있는 사용률이 낮은 인스턴스를 식별하고 보고합니다.

계정 중심 권장 사항

- 계정 정리: 계정 수준에서 AMS는 사용되지 않는 EBS 볼륨, 중복 CloudTrail 추적, 미사용 리소스가 있는 빈 계정 등을 식별하고 정리를 위한 권장 사항을 제공합니다.
- SLA 권장 사항: 또한 AMS는 Plus 및 Premium 계정을 정기적으로 검토하고 계정에 적합한 SLA 수준을 선택할 것을 권장합니다.
- AMS 자동화 최적화: AMS는 AMS 서비스를 제공하는 데 사용되는 AMS 자동화 및 인프라를 지속적으로 최적화합니다.

고객에게 제시 및 계획 지원

AMS는 주요 고객 이해관계자와 함께 월별 비즈니스 검토(MBRs)를 수행하고 잠재적 비용 절감과 함께 식별된 비용 절감 방법, 메커니즘 및 권장 사항을 제시합니다. 또한 필요한 변경 사항을 계획하기 위해 고객과 협력합니다.

권장 사항 구현 지원 및 비용 영향 측정

AMS는 비용 영향 및 최적화 변경을 달성하고 측정하는 데 도움이 됩니다.

권장 변경 사항의 애플리케이션 영향, 위험 및 성공 기준을 평가하고 AMS 콘솔을 통해 적절한 변경 요청(RFCs)을 제기합니다. AMS는 사용자와 협업하고 관리형 계정에서 비용 최적화와 관련된 변경 사항을 구현합니다. AMS는 비용 영향을 측정하고 월별 비즈니스 검토(MBRs)에 실현된 절감액을 포함합니다.

비용 최적화 책임 매트릭스

AMS 비용 최적화에 대한 책임.

비용 최적화 RACI

활동	Customer	AMS
비용 절감 권장 사항 컴파일 및 보고서 준 비	정보	R

활동	Customer	AMS
비용 절감 보고서 제 시	C	R
비용 절감 과 관련된 변경 계획	R	C
변경 영향 및 위험 평가	R	C
변경 사 항 구현 RFCs 중 가	R	C
RFCs 검 토 및 변 경 사항 구현	C	R
애플리케 이션 테스 트 및 변 경 구현 검증	R	C
변경 후 비용에 미 치는 영향 측정 및 고객에게 제시	정보	R

AWS Managed Services의 서비스 시간

Feature	AMS 고급
	프리미엄 티어
서비스 요청	24/7
인시던트 관리(P2-P3)	24/7
백업 및 복구	24/7
패치 관리	24/7
모니터링 및 알림	24/7
자동 변경 요청(RFC)	24/7
자동이 아닌 변경 요청(RFC)	24/7
클라우드 서비스 제공 관리자(CSDM)	월요일~금요일: 08:00~17:00, 현지 업무 시간

AWS Managed Services에 대한 도움말 보기

AMS는 하루 24시간, 주 7일, 1년 365일(계정에 적용된 AMS 서비스 수준 계약에 따라) Incident Management, Service Request Management 및 Change Management를 지원합니다.

관리형 환경에 영향을 미치는 AWS 또는 AMS 서비스 성능 문제를 보고하려면 AMS 콘솔을 사용하여 인시던트 보고서를 제출합니다. 자세한 내용은 [인시던트 보고를 참조하세요](#). AMS 인시던트 관리에 대한 일반적인 정보는 [인시던트 대응](#)을 참조하세요.

정보나 조언을 요청하거나 AMS에서 추가 서비스를 요청하려면 AMS 콘솔을 사용하여 서비스 요청을 제출합니다. 자세한 내용은 [서비스 요청 생성을 참조하세요](#). AMS 서비스 요청에 대한 일반 정보는 [서비스 요청 관리](#)를 참조하세요.

AWS Managed Services의 계획된 이벤트 관리

AWS Managed Services(AMS) 계획된 이벤트 관리(PEM)는 AMS 서비스 상품입니다. PEM은 고객 이벤트 및 프로젝트 중에 AMS 서비스를 사용하여 참여, 조정 및 지원합니다. PEM은 PEM 이벤트 또는 프로젝트의 합의된 범위 및 일정에 맞는 관련 RFCs 세트를 조정하는 데 도움이 됩니다.

AMS PEM 기준

계획된 이벤트는 범위 제한 및 시간 제한 프로젝트입니다. AMS는 사용자가 제공하는 세부 정보(계획 및 범위, 예상 결과, AMS 작업이 수행할 것으로 예상되는 변경 사항 포함)를 사용하여 PEM 활동 중에 사용자를 효과적으로 지원합니다. 그런 다음 클라우드 아키텍트(CAs)는 PEM 활동의 완전성, 기술 구현 및 AMS 운영 참여를 검토하고 평가합니다. CA 검토 후 AMS 작업은 계획을 검토하고 운영 팀 참여를 위해 클라우드 서비스 제공 관리자(CSDM)와 조정합니다.

PEM 유형

사용 가능한 PEM 유형은 다음과 같습니다.

- 게임데이
 - 운영 게임데이: 프로세스, 사람 및 시스템의 통합을 검증하는 것을 목표로 운영 대응에 대한 시나리오 기반 게임 접근 방식입니다.
 - Security Gameday: 시나리오 기반 게임 접근 방식을 사용하여 시스템, 프로세스 및 인력의 통합을 평가하는 보안 인시던트 대응 전략입니다.
- BYOEPS: AMS "bring your own endpoint security"(BYOEPS) 기능을 사용하여 기본 Trend Micro Deep Security 에이전트를 선호하는 엔드포인트 보안 솔루션 또는 사용자 지정 Trend Micro 라이선스로 대체합니다. 자세한 내용은 [AMS에서 자체 EPS 사용](#) 단원을 참조하십시오.
- 재해 복구: 재해 복구 이벤트에는 계획된 DR 활동 중에 사용자를 지원하는 AMS가 포함됩니다. 자세한 내용은 [재해 복구 계획](#) 단원을 참조하십시오.
- 고객 보안 이벤트: 계획된 보안 이벤트. 예를 들어 루트 사용자 활동 및 침투 테스트입니다.
- 마이그레이션 지원: 계획된 온보딩 및 마이그레이션 활동을 지원합니다.

이 워크플로는 AMS 지원과 관련하여 계획된 이벤트 및 마이그레이션 활동을 조정하기 위해 AMS와의 협업을 용이하게 합니다. RFCs의 우선 순위 실행의 경우 OOD(Options on Demand) 참여를 사용하는 것이 가장 좋습니다. 자세한 내용은 [온디맨드 작업](#) 단원을 참조하십시오.

AMS PEM 프로세스

PEM 프로세스는 다음 단계로 구성됩니다.

- PEM 시작: CSDM과 협력하여 계획된 이벤트에 대한 목표를 정의하고 AMS 작업에 필요한 사항을 결정합니다. AMS CAs PEM 계획의 기술적 측면을 검토합니다. CAs는 AMS 보안 및 운영 부서와 협력하여 규정 준수, 실행 최적화 및 자동화를 수행하고 사전 PEM 실행 작업 및 결과물을 정의합니다. 그런 다음 CSDM이 PEM 티켓을 생성하고 AMS에 프로젝트 정보와 기술 세부 정보를 제공합니다. AMS 운영 팀이 리소스를 계획하고, 기술 검토를 제공하고, 할당하는 데 걸리는 리드 타임은 14일입니다.
- PEM 검토: AMS 운영 팀이 PEM 요청을 검토하고 CSDM과 협력하여 PEM 계획의 정보가 정확하고 완전한지 확인합니다.
- PEM 수락: AMS는 제공된 정보를 검토하고 PEM 활동 중에 지원 수준이 무엇인지 CSDM에 전달합니다. PEM에 전체 정보가 포함되어 있고 CSDM이 작업 범위에 동의하는 경우 PEM이 승인됩니다.
- 준비 및 실행: AMS는 PEM이 시작되기 전에 필요한 작업이 완료되었는지 확인하고 내부 및 고객 커뮤니케이션을 용이하게 합니다. AMS는 PEM 계획이 올바르게 실행되고 상태 및 진행 상황 보고를 제공하는지 확인합니다.

PEM FAQs

PEM 이벤트 중에 AMS를 RFC/서비스 요청(SR)과 연결하려면 어떻게 해야 하나요?

- 형식의 RFC/SR 제목 줄에서 CSDM이 공유하는 PEM ID를 사용합니다 **PEM-ID**.
- 서비스 요청(SR)을 생성하여 사용 사례를 논의하거나 계획된 이벤트에 대한 질문을 할 수도 있습니다. SR을 사용하는 경우 PEM이 유효하지 않아도 됩니다.

PEM 관련 RFC가 제출되면 어떤 검증이 수행되나요?

- 계정 ID가 PEM에 나열되어 있는지 확인합니다.
- 제공된 시작일과 종료일 사이에 PEM 상태가 승인되고 활성 상태인지 확인합니다.

PEM 요청에 대한 SLAs 또는 SLOs 있습니까?

- PEMs은 SLAs 또는 SLOs와 연결되지 않습니다.
- PEM 관련 작업 항목(RFC/서비스 요청)에 SLOs 대한 SLAs 및 SLO는 AMS SLOs 의해 정의됩니다.

자세한 내용은 [AMS 서비스 수준 목표\(SLOs\)](#).

서비스 요청(SR)을 통해 PEM을 생성할 수 있나요?

- 아니요. PEM 생성은 Cloud Service Delivery Manager(CSDM)에서 관리해야 합니다.

네트워크 아키텍처

AWS Managed Services(AMS)는 두 가지 네트워크 아키텍처를 제공합니다.

- 다중 계정 랜딩 존(MALZ):는 별도의 멤버 계정에 배포된 워크로드에 대한 공유 계정의 액세스, 엔드포인트 보안, 네트워킹과 같은 공통 서비스를 제공합니다.
- 단일 계정 랜딩 존(SALZ): 액세스, 엔드포인트 보안, 네트워킹과 같은 공통 서비스가 워크로드와 동일한 계정에 배포되는 자체 포함 계정을 제공합니다. 높은 AWS 비용이 발생하므로 높은 수준의 격리가 필요한 워크로드에 권장됩니다.

MALZ 네트워크 아키텍처

다중 계정 랜딩 존 네트워크 아키텍처 정보

AWS Managed Services(AMS) 다중 계정 랜딩 존(MALZ)에 대한 온보딩 프로세스를 시작하기 전에 AMS가 사용자를 대신하여 생성하는 기본 아키텍처 또는 랜딩 존, 해당 구성 요소 및 함수를 이해하는 것이 중요합니다.

AMS 다중 계정 랜딩 존은 인증, 보안, 네트워킹 및 로깅을 용이하게 하기 위해 인프라로 사전 구성된 다중 계정 아키텍처입니다.

Note

예상 비용은 [AMS 다중 계정 랜딩 존 환경 기본 구성 요소를](#) 참조하세요.

주제

- [서비스 리전](#)
- [조직 단위](#)
- [서비스 제어 정책 및 AWS Organization](#)

다음 다이어그램은 계정 구조와 인프라가 각 계정으로 분리되는 방법을 개략적으로 설명합니다.

서비스 리전

AMS 다중 계정 랜딩 존 내의 모든 리소스는 Active Directory 및 Transit Gateway의 현재 교차 리전 제한으로 인해 선택한 단일 AWS 리전 내에 배포됩니다.

조직 단위

일반적인 AMS 다중 계정 랜딩 존은 4개의 최상위 조직 단위(OU)로 구성됩니다.

- 핵심 조직 단위(OU)(계정을 그룹화하여 단일 단위로 관리하는 데 사용됨)
- 애플리케이션 OU
- 고객 관리형 OU
- 가속화된 OU

또한 AMS 관리형 다중 계정 랜딩 존을 사용하면 AWS 계정을 그룹화 및 구성하기 위한 사용자 지정 OUs를 생성하고 사용자 지정 SCPs를 해당 계정과 연결할 수 있습니다. 이에 대한 예제는 각각 [관리 계정 | 사용자 지정 OUs 및 관리 계정 생성 | 사용자 지정 SCP 생성\(검토 필요\)](#)을 참조하세요. AMS는 가속화, 애플리케이션 > 관리형, 애플리케이션 > 개발, 고객 관리형 등 새로운 OU와 계정을 요청할 수 OUs 있는 4가지 기존 OUs를 제공합니다.

- OU 가속화:

AMS 다중 계정 랜딩 존(MALZ)의 최상위 OU입니다. 이 OU의 계정은 RFC(배포 | 관리형 랜딩 존 | 관리 계정 | Accelerate 계정 생성, 변경 유형 ID: ct-2p93tyd5angmi)를 사용하여 AMS에 의해 프로비저닝됩니다. 이러한 가속화된 애플리케이션 계정에서는 모니터링 및 알림, 인시던트 관리, 보안 관리, 백업 관리와 같은 가속화된 운영 서비스를 활용할 수 있습니다. 자세한 내용은 [AMS Accelerate 계정을](#) 참조하세요.

- 애플리케이션 > 관리형 OU:

애플리케이션 OU의 하위 조직 단위에서 계정은 모든 운영 작업을 포함하여 AMS에 의해 완전히 관리됩니다. 운영 작업에는 서비스 요청 관리, 인시던트 관리, 보안 관리, 연속성 관리, 패치 관리, 비용 최적화, 모니터링 및 이벤트 관리가 포함됩니다. 이러한 작업은 인프라 관리를 위해 수행됩니다. AWS 조직에서 중첩된 OUs의 최대 한도에 도달할 때까지 필요에 따라 여러 하위 OUs를 생성할 수 있습니다. 자세한 내용은 [AWS Organizations 할당량을](#) 참조하세요.

- 애플리케이션 > 개발 OU:

AMS 관리형 랜딩 존에 있는 애플리케이션 OU의 하위 OU에서 계정은 AMS 변경 관리 프로세스 외부에서 AWS 리소스를 프로비저닝하고 업데이트할 수 있는 승격된 권한을 제공하는 [개발자 모드](#) 계정입니다. 또한 이 OU는 필요에 따라 새 하위 OU 생성을 지원합니다.

- 고객 관리형 OU:

이는 AMS 다중 계정 랜딩 존의 최상위 OU입니다. 이 OU의 계정은 RFC가 있는 AMS에서 프로비저닝됩니다. 이러한 계정에서 워크로드 및 AWS 리소스의 운영은 사용자의 책임입니다. 또한 이 OU는 필요에 따라 새 하위 OU 생성을 지원합니다.

가장 좋은 방법은 이러한 OUs 및 사용자 지정 요청 하위 OUs의 계정을 기능 및 정책에 따라 그룹화하는 것입니다.

서비스 제어 정책 및 AWS Organization

AWS는 AWS Organization에서 권한 관리를 위한 서비스 제어 정책(SCPs)을 제공합니다. SCPs는 사용자가 어떤 OUs에서 수행할 수 있는 작업에 대한 추가 가드레일을 정의하는 데 사용됩니다. 기본적으로 AMS는 서로 다른 기본 OU 수준에서 보호를 제공하는 관리 계정에 배포된 SCPs 세트를 제공합니다. SCP 제한에 대해서는 CSDM에 문의하십시오.

사용자 지정 SCPs 생성하여 특정 OUs. 변경 유형 ct-33ste5yc7hprs를 사용하여 관리 계정에서 요청할 수 있습니다. 그런 다음 AMS는 요청된 사용자 지정 SCPs 대상 OUs에 적용하기 전에 검토합니다. 예제는 [관리 계정 | 사용자 지정 OUs](#). <https://docs.aws.amazon.com/managedservices/latest/ctref/deployment-managed-management-account-create-custom-scp-review-required.html>

단일 MALZ 또는 여러 MALZs 선택

다음 표에서는 단일 다중 계정 랜딩 존(MALZ)과 여러 다중 계정 랜딩 존(예: 두 개의 다중 계정 랜딩 존 - Prod 및 비Prod)을 결정할 때 몇 가지 높은 수준의 고려 사항을 제공합니다. 일반적으로 선택은 개별 요구 사항, 법적 요구 사항 및 운영 관행에 따라 달라집니다.

단일 다중 계정 랜딩 존과 다중 계정 랜딩 존 비교

개체	단일 AMS 랜딩 존	여러(2개 이상) 랜딩 존
기본 비용	매월 약 3,000 USD로 더 낮고 최적화되었습니다.	더 높으면 환경당 약 3,000 USD의 추가 비용이 발생합니다.
결제	단일 Billing/ Management 계정으로 인한 단일 청구서.	각 다중 계정 랜딩 존에 대해 청구서를 구분합니다. 현재 AWS Org는 단일 청

개체	단일 AMS 랜딩 존	여러(2개 이상) 랜딩 존
		구서가 있는 다중 관리 계정을 지원하지 않습니다.
기존 예약 인스턴스(RIs)의 이식성	낮음. AWS RIs는 현재 여러 결제 계정에서 전환할 수 없습니다. 다중 계정 랜딩 존에 대해 기존 RIs의 용도를 변경합니다.	더 낮습니다. 모든 다중 계정 랜딩 존에서 RIs 용도를 변경하고 배포합니다.
제품 계층화 할인	높음 볼륨 할인을 참조하세요.	낮음. 볼륨 할인을 참조하세요.
초기 설정 오버헤드(프로젝트/마이그레이션 타임라인)	낮음. Active Directory, 네트워킹 및 SSO(Single Sign-On) 통합은 한 번만 가능합니다.	높음 모든 랜딩 존에 대해 Active Directory, 네트워크 통합 및 SSO 통합을 수행합니다. 이로 인해 마이그레이션 프로젝트가 지연될 수 있습니다.
공통 서비스 구성 가능성	낮은 노력. DNS, 백업, 모니터링, 로깅 등과 같은 공통/공유 서비스를 구성합니다.	높은 노력. 공통 인프라 또는 서비스의 위치를 해결하려면 추가 계획이 필요합니다. 트래픽이 각 랜딩 존의 여러 전송 게이트웨이(TGWs)를 통과하면 추가 비용이 발생할 수 있습니다.
확장성	중간. AMS의 현재 실제 한도는 다중 계정 랜딩 존당 150개입니다. 동일한 계정에서 애플리케이션을 실행하는 여러 팀 또는 공급업체는 서로 다른 팀이 소유한 스택에 액세스할 수 있습니다. ServiceNow 계층에서 애플리케이션별 스택에 대한 액세스를 제어하여(AMS ServiceNow Connector 애플리케이션을 통합하고 태그를 사용하여) 이러한 제한을 완화할 수 있습니다. AMS 기술 제공 관리자(TDMs) 또는 클라우드 아키텍트(CAs)에게 이를 구현하는 방법을 문의하십시오.	높음 여러 다중 계정 랜딩 존을 활용하여 계정을 분산하는 동시에 계정 또는 애플리케이션 수준의 분리를 달성할 수 있습니다. 많은 수의 계정을 관리하면 운영 또는 비용 오버헤드가 발생할 수 있습니다.

개체	단일 AMS 랜딩 존	여러(2개 이상) 랜딩 존
운영 위험	(중속) 낮음. 운영 통합 및 준비는 한 번만 가능합니다. 프로세스 드리프트의 가능성이 줄어듭니다.	(중속) 낮음. 여러 통합 및 운영 활동. 일정 기간 동안 여러 랜딩 존의 드리프트는 운영 위험을 초래할 수 있습니다.
다중 AWS 리전	단일 AWS 리전. AMS 다중 계정 랜딩 존은 단일 AWS 리전으로 제한됩니다. 여러 AWS 리전을 확장하려면 여러 다중 계정 랜딩 존을 사용합니다.	다중 AWS 리전. 다중 계정 랜딩 존이 여러 개인 경우 각 MALZ를 한 리전에 배포하고 전송 게이트웨이(TGW) 피어링을 사용하여 상호 연결할 수 있습니다.
계정 마이그레이션 또는 이동성	예. 동일한 AWS 조직 내에서 한 OU에서 다른 OU로 계정을 이동할 수 있습니다.	아니요. AMS는 랜딩 존, 즉 AWS Organizations 간 계정 마이그레이션을 지원하지 않습니다. 워크로드는 전송 게이트웨이(TGW) 또는 VPC 피어링을 통해 랜딩 존에 도달할 수 있습니다.
변경 관리	중간. TGW, Active Directory(AD) 또는 아웃바운드(송신)와 같은 일반적인 구성 요소를 파괴적으로 변경하면 다중 계정 랜딩 존의 모든 워크로드에 영향을 미칠 수 있습니다. 그러나 AMS 관리형 구성 요소의 변경 사항은 내부적으로 테스트되며 롤링 업데이트에서 푸시됩니다.	낮음. TGW, AD 또는 아웃바운드(송신)와 같은 일반적인 구성 요소를 파괴적으로 변경하면 해당 특정 다중 계정 랜딩 존의 워크로드에만 영향을 미칠 수 있습니다.
데이터 및 액세스 제어	(중속) Prod 워크로드와 Non-Prod 워크로드를 위해 다양한 온프레미스 ADs 및 네트워크에 연결하려는 경우 제어가 낮습니다. SAML 페더레이션, TGW 도메인 및 보안 그룹(SGs)도 필요한 제어를 구현하는 데 도움이 될 수 있습니다.	(중속) Prod 워크로드와 Non-Prod 워크로드를 위해 다양한 온프레미스 ADs 및 네트워크에 연결하려는 경우 높은 제어가 가능합니다. 엄격한 규정 준수 요구 사항에 대해 별도의 랜딩 존을 사용합니다.

개체	단일 AMS 랜딩 존	여러(2개 이상) 랜딩 존
규정 준수 및 보안	(종속) 재료 워크로드와 비 재료 워크로드를 완전히 분리해야 하는 엄격한 규정 준수 요구 사항이 있는 경우 낮음. AMS 표준 예방 및 탐지 제어가 마련되어 있습니다.	(종속) 다중 계정 랜딩 존이 높으면 재료 워크로드와 비 재료 워크로드를 완전히 분리하여 엄격한 규정 준수 요구 사항을 달성하는 데 도움이 될 수 있습니다. AMS 표준 예방 및 탐지 제어가 마련되어 있습니다.

권장 사항: 엄격한 규정 준수 또는 다중 리전 요구가 없으면 단일 AMS 다중 계정 랜딩 존부터 시작하여 비용, 보안, 운영 우수성 및 마이그레이션 복잡성 간에 균형이 잘 맞습니다. 계정 또는 비즈니스 제약이 발생하는 경우 언제든지 추가 랜딩 존을 설정할 수 있습니다.

단일 다중 계정 랜딩 존과 다중 다중 계정 랜딩 존 FAQs

단일 다중 계정 랜딩 존 또는 다중 계정 랜딩 존을 설정하기로 선택할 때 자주 묻는 몇 가지 질문:

Q1: 계정 제한 또는 비즈니스 제약이 발생하는 경우 단일 다중 계정 랜딩 존으로 시작하여 다중 계정 랜딩 존으로 이동할 수 있습니까?

A: 예. 언제든지 다른 다중 계정 랜딩 존을 설정하도록 선택할 수 있습니다.

- 새 결제자 계정을 설정해야 합니다(현재 AWS는 단일 AWS 조직에서 다중 결제자 계정을 지원하지 않음).
- 다중 계정 랜딩 존 기본 빌드는 다중 계정 랜딩 존 설문지를 작성한 후 최대 2주가 걸립니다.
- 모든 다중 계정 랜딩 존은 월 최대 3,000 USD의 실행 비용이 추가됩니다.
- 새 MALZ에 대해 설정하려면 N/W, AD, DNS 및 SSO 통합이 필요합니다.
- 모든 예약 인스턴스(RIs), 비용 절감형 플랜은 새 다중 계정 랜딩 존에 대해 설정해야 합니다(RIs는 이전할 수 없음).
- AMS 다중 계정 랜딩 존은 AWS 조직과 같은 다중 계정 랜딩 존 계정 간 계정 마이그레이션을 지원하지 않습니다. 그러나 표준 마이그레이션 방법을 사용하면 한 계정에서 다른 계정으로 애플리케이션을 이동할 수 있습니다.

Q2: 기본/공유 인프라에 대한 MALZ 업데이트/변경 및 고객에 대한 위험 정량화에 대한 AMS 접근 방식은 무엇입니까? 프로세스에 래핑되는 보증에 대한 세부 정보를 제공합니다. 고객은 MALZ 업데이트/변

경이 고객에게 영향을 미치지 않을 것이라고 어떻게 확신하나요? 중단을 방지하기 위해 고객이 취해야 할 조치가 있나요?

A: AMS는 고객의 환경에 대한 변경 사항을 정의, 검토, 예약 및 실행할 수 있는 내부 도구를 사용하여 엄격한 변경 방법론을 따릅니다.

업데이트 릴리스 프로세스는 고객 환경에 릴리스하기 전에 코드 검토, 통합 테스트, 감마 및 베타 환경에서의 배포, 베타 및 감마 환경에서의 추가 베이킹 시간 및 테스트를 적용합니다. 모든 릴리스에는 롤백 절차가 포함되며 릴리스 팀과 변경을 생성하고 요청한 팀이 면밀히 모니터링합니다. 릴리스의 범위는 AMS가 소유하고 프로비저닝한 스택으로 제한됩니다. 평균적으로 매주 최소 1개의 릴리스를 실행합니다.

또한 다음과 같습니다.

- AMS SLA가 적용됩니다. AMS 서비스 설명에 따라 인시던트 발생 게시물 공유 인프라 유지 관리 활동은 해결 또는 크레딧을 위해 권한이 부여된 SLA를 준수합니다.
- 고객은 공통 인프라 중단을 방지하기 위해 특별한 예방 조치를 취할 필요가 없습니다. 고객은 AWS Org 또는 Core OU 계정에서 읽기 전용 권한을 보유하므로 MALZ 코어 환경을 파괴적으로 변경할 수 없습니다. 코어 인프라에 대한 모든 고객의 요청에는 AMS 검토 및 승인이 필요합니다.
- 고객은 앱 OU 수준에서 변경 사항을 전파하기 전에 개별 비프로드 계정 수준에서 SCPs/역할과 같은 특정 조직 수준 변경 사항을 테스트할 수 있습니다. AMS 로드맵에서는 여러 APP OUs(2020년 2분기)를 허용하므로 일부 ORG 수준 변경의 위험을 더욱 완화할 수 있습니다. MALZ 팀은 고객 소유권의 명확한 분리와 별도의 제어를 보장하기 위해 “빌드 모드” 계정에 대해 별도의 OU를 이미 릴리스했습니다.
- 이 중 대부분은 AMS가 효과적이고 효율적인 방식으로 워크로드를 운영할 수 있도록 허용하는 변경 사항이며 반드시 고객의 워크로드에 영향을 미치지 않습니다. AMS가 공유된 인프라 변경이 고객의 워크로드에 영향을 미칠 수 있다고 생각하는 경우 고객의 변경 기간에 맞춰 조정됩니다.

다음과 같은 경우 여러 다중 계정 랜딩 존으로 시작하는 높은 수준의 권장 사항입니다.

- 특정 규정 준수를 달성하는 데 도움이 되는 경우.
- 다중 리전을 사용해야 하는 경우.
- 온프레미스 ADs 및 Network for Prod/Material과 Non-Prod/Non-Material 워크로드가 다른 경우 워크로드를 b/w로 명확하게 분리합니다.

다중 계정 랜딩 존 계정

주제

- [관리 계정](#)
- [네트워킹 계정](#)
- [공유 서비스 계정](#)
- [로그 아카이브 계정](#)
- [보안 계정](#)
- [애플리케이션 계정 유형](#)
- [AMS 도구 계정\(워크로드 마이그레이션\)](#)

관리 계정

관리 계정은 AMS로 온보딩을 시작할 때 초기 AWS 계정입니다. AWS Organizations를 관리 계정(모든 멤버 계정의 요금을 지불하는 지급인 계정이라고도 함)으로 활용하며, 이를 통해 계정은 멤버 계정을 생성하고 재무적으로 관리할 수 있습니다. 여기에는 AWS 랜딩 존(ALZ) 프레임워크, 계정 구성 스택 세트, AWS 조직 서비스 제어 정책(SCPs) 등이 포함됩니다.

관리 계정 사용에 대한 자세한 내용은 [관리 계정 모범 사례를 참조하세요](#).

다음 다이어그램은 관리 계정에 포함된 리소스에 대한 개략적인 개요를 제공합니다.

관리 계정의 리소스

위의 표준 서비스 외에는 온보딩 중에 관리 계정에 추가 AWS 리소스가 생성되지 않습니다. AMS에 온보딩하는 동안 다음 입력이 필요합니다.

- 관리 계정 ID: 사용자가 처음 생성한 AWS 계정 ID입니다.
- 코어 계정 이메일: 네트워킹, 공유 서비스, 로깅 및 보안 계정과 같은 각 코어 계정과 연결할 이메일을 제공합니다.
- 서비스 리전: AMS 랜딩 존의 모든 리소스가 배포될 AWS 리전을 제공합니다.

네트워킹 계정

네트워킹 계정은 AMS 다중 계정 랜딩 존 계정, 온프레미스 네트워크, 인터넷으로의 송신 트래픽 간의 네트워크 라우팅을 위한 중앙 허브 역할을 합니다. 또한 이 계정에는 AMS 엔지니어가 AMS 환경의 호

스트에 액세스할 수 있는 진입점인 퍼블릭 DMZ 접속이 포함되어 있습니다. 자세한 내용은 아래 네트워크 계정의 다음 상위 수준 다이어그램을 참조하세요.

네트워크 계정 아키텍처

다음 다이어그램은 계정 간 네트워크 트래픽 흐름을 보여주는 AMS 다중 계정 랜딩 존 환경을 보여주며 가용성이 높은 설정의 예입니다.

AMS는 표준 템플릿과 온보딩 중에 제공된 선택한 옵션을 기반으로 네트워크의 모든 측면을 구성합니다. 표준 AWS 네트워크 설계가 AWS 계정에 적용되고 VPC가 자동으로 생성되어 VPN 또는 Direct Connect를 통해 AMS에 연결됩니다. Direct Connect에 대한 자세한 내용은 [AWS Direct Connect](#)를 참조하세요. 표준 VPCs에는 DMZ, 공유 서비스 및 애플리케이션 서브넷이 포함됩니다. 온보딩 프로세스 중에 필요에 맞게 추가 VPCs를 요청하고 생성할 수 있습니다(예: 고객 부서, 파트너). 온보딩 후 네트워크 다이어그램, 즉 네트워크 설정 방법을 설명하는 환경 문서가 제공됩니다.

Note

모든 활성 서비스의 기본 서비스 제한 및 제약 조건에 대한 자세한 내용은 [AWS 서비스 제한 설명서를 참조하세요](#).

네트워크 설계는 Amazon "[최소 권한 원칙](#)"을 기반으로 구축되었습니다. 이를 위해 신뢰할 수 있는 네트워크에서 들어오는 트래픽을 제외한 모든 트래픽, 수신 및 송신을 DMZ를 통해 라우팅합니다. 유일하게 신뢰할 수 있는 네트워크는 VPN 및/또는 AWS Direct Connect(DX)를 사용하여 온프레미스 환경과 VPC 간에 구성된 네트워크입니다. 접속 인스턴스를 사용하여 액세스 권한이 부여되므로 프로덕션 리소스에 직접 액세스할 수 없습니다. 모든 애플리케이션과 리소스는 퍼블릭 로드 밸런서를 통해 연결할 수 있는 프라이빗 서브넷 내에 있습니다. 퍼블릭 송신 트래픽은 송신 VPC(네트워크 계정)의 NAT 게이트웨이를 통해 인터넷 게이트웨이로 흐른 다음 인터넷으로 흐릅니다. 또는 트래픽이 VPN 또는 Direct Connect를 통해 온프레미스 환경으로 흐를 수 있습니다.

AMS 다중 계정 랜딩 존 환경에 대한 프라이빗 네트워크 연결

AWS는 가상 프라이빗 네트워크(VPN) 연결 또는 AWS Direct Connect를 통한 전용 라인을 통해 프라이빗 연결을 제공합니다. 다중 계정 환경의 프라이빗 연결은 다음에 설명된 방법 중 하나를 사용하여 설정됩니다.

- Transit Gateway를 사용한 중앙 집중식 엣지 연결
- Direct Connect(DX) 및/또는 VPN을 계정 Virtual Private Cloud(VPCs)에 연결

전송 게이트웨이를 사용한 중앙 집중식 엣지 연결

AWS Transit Gateway는 VPCs와 온프레미스 네트워크를 단일 게이트웨이에 연결할 수 있는 서비스입니다. 전송 게이트웨이(TGW)를 사용하여 기존 엣지 연결을 통합하고 단일 수신/송신 지점을 통해 라우팅할 수 있습니다. 전송 게이트웨이는 AMS 다중 계정 환경의 네트워킹 계정에 생성됩니다. 전송 게이트웨이에 대한 자세한 내용은 [AWS Transit Gateway](#)를 참조하세요.

AWS Direct Connect(DX) 게이트웨이는 전송 가상 인터페이스를 통해 전송 게이트웨이에 연결된 VPCs 또는 VPNs에 DX 연결을 연결하는 데 사용됩니다. Direct Connect 게이트웨이를 전송 게이트웨이와 연결합니다. 그런 다음 Direct Connect 게이트웨이에 대한 AWS Direct Connect 연결을 위한 전송 가상 인터페이스를 생성합니다. DX 가상 인터페이스에 대한 자세한 내용은 [AWS Direct Connect 가상 인터페이스를 참조하세요](#).

이 구성을 사용하면 다음과 같은 이점이 있습니다. 다음을 할 수 있습니다.

- 동일한 AWS 리전에 있는 여러 VPCs 또는 VPNs에 대한 단일 연결을 관리합니다.
- 온프레미스에서 AWS로, AWS에서 온프레미스로 접두사를 알립니다.

Note

AWS 서비스에서 DX를 사용하는 방법에 대한 자세한 내용은 Resiliency Toolkit 섹션 [Classic](#)을 참조하세요. 자세한 내용은 [Transit Gateway 연결을 참조하세요](#).

연결 복원력을 높이려면 서로 다른 AWS Direct Connect 위치의 전송 가상 인터페이스를 Direct Connect 게이트웨이에 두 개 이상 연결하는 것이 좋습니다. 자세한 내용은 [AWS Direct Connect 복원력 권장 사항을 참조하세요](#).

계정 VPCs에 DX 또는 VPN 연결

이 옵션을 사용하면 AMS 다중 계정 랜딩 존 환경의 VPCs가 Direct Connect 또는 VPN에 직접 연결됩니다. 트래픽은 전송 게이트웨이를 통과하지 않고 VPCs에서 Direct Connect 또는 VPN으로 직접 흐릅니다.

네트워킹 계정의 리소스

네트워킹 계정 다이어그램에 표시된 대로 다음 구성 요소가 계정에 생성되며 입력이 필요합니다.

네트워킹 계정에는 송신 VPCs와 경계 VPC라고도 하는 DMZ VPC라는 두 개의 VPC가 포함되어 있습니다.

AWS Network Manager

AWS Network Manager는 AMS에 대한 추가 비용 없이 전송 게이트웨이(TGW) 네트워크를 시각화할 수 있는 서비스입니다. AWS 리소스와 온프레미스 네트워크에서 중앙 집중식 네트워크 모니터링, 토폴로지 다이어그램과 지리적 맵에서 프라이빗 네트워크의 단일 글로벌 보기, 바이트 입/출력, 패킷 입/출력, 삭제된 패킷, 토폴로지, 라우팅 및 업/다운 연결 상태 변경 알림과 같은 사용자 지표를 제공합니다. 자세한 내용은 [AWS Network Manager](#) 단원을 참조하세요.

다음 역할 중 하나를 사용하여이 리소스에 액세스합니다.

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

송신 VPC

송신 VPC는 주로 인터넷으로의 송신 트래픽에 사용되며 최대 3개의 가용 영역(AZs)에 있는 퍼블릭/프라이빗 서브넷으로 구성됩니다. NAT(Network Address Translation) 게이트웨이는 퍼블릭 서브넷에 프로비저닝되고 TGW(Transit Gateway) VPC 연결은 프라이빗 서브넷에 생성됩니다. 모든 네트워크의 송신 또는 아웃바운드 인터넷 트래픽은 TGW를 통해 프라이빗 서브넷을 통해 들어오는 다음 VPC 라우팅 테이블을 통해 NAT로 라우팅됩니다.

퍼블릭 서브넷에 퍼블릭 애플리케이션을 포함하는 VPCs의 경우 인터넷에서 발생하는 트래픽은 해당 VPC 내에 포함됩니다. 반환 트래픽은 TGW 또는 송신 VPC로 라우팅되지 않고 VPC의 인터넷 게이트웨이(IGW)를 통해 다시 라우팅됩니다.

Note

네트워킹 VPC CIDR 범위: VPC를 생성할 때 Classless Inter-Domain Routing(CIDR) 블록의 형태로 VPC에 대한 IPv4 주소 범위를 지정해야 합니다. 예: 10.0.16.0/24. 이것은 VPC의 기본 CIDR 블록입니다.

AMS 다중 계정 랜딩 존 팀은 향후 다른 리소스/어플라이언스가 배포될 경우를 대비하여 일부 버퍼를 제공하기 위해 24(IP 주소 증가)의 범위를 권장합니다.

Managed Palo Alto 송신 방화벽

AMS는 다중 계정 랜딩 존 환경(퍼블릭 서비스 제외)의 모든 네트워크에 대해 인터넷 바운드 아웃바운드 트래픽을 필터링할 수 있는 Managed Palo Alto 송신 방화벽 솔루션을 제공합니다. 이 솔루션은 업계 최고의 방화벽 기술(Palo Alto VM-300)과 AMS의 인프라 관리 기능을 결합하여 규정을 준수하는 운영 환경 내에서 인프라를 배포, 모니터링, 관리, 확장 및 복원합니다. Palo Alto Networks를 포함한 타사는 방화벽에 액세스할 수 없으며 AMS 엔지니어만 관리합니다.

트래픽 제어

관리형 아웃바운드 방화벽 솔루션은 백업 및 패치와 같은 서비스의 AMS 필수 도메인과 정의된 도메인으로 구성된 도메인 허용 목록을 관리합니다. 아웃바운드 인터넷 트래픽이 방화벽으로 라우팅되고, 세션이 열리고, 트래픽이 평가되고, 허용된 도메인과 일치하면 트래픽이 대상으로 전달됩니다.

아키텍처

관리형 송신 방화벽 솔루션은 가용 영역(AZs) 수에 따라 2~3개의 방화벽이 배포되는고가용성 모델을 따릅니다. 이 솔루션은 기본 송신 VPC의 IP 공간 일부를 활용하지만 방화벽 관리에 필요한 추가 리소스에 대해 VPC 확장(/24)도 프로비저닝합니다.

네트워크 흐름

상위 수준에서 퍼블릭 송신 트래픽 라우팅은 송신 VPC에서 인터넷으로 트래픽이 라우팅되는 방식을 제외하고 동일하게 유지됩니다.

1. 인터넷으로 향하는 송신 트래픽은 VPC 라우팅 테이블을 통해 Transit Gateway(TGW)로 전송됩니다.
2. TGW는 TGW 라우팅 테이블을 통해 트래픽을 송신 VPC로 라우팅합니다.
3. VPC는 프라이빗 서브넷 라우팅 테이블을 통해 트래픽을 인터넷으로 라우팅합니다.
 - a. 기본 다중 계정 랜딩 존 환경에서 인터넷 트래픽은 네트워크 주소 변환(NAT) 게이트웨이로 직접 전송됩니다. 관리형 방화벽 솔루션은 대신 기본 경로(0.0.0.0/0)가 방화벽 인터페이스를 가리키도록 프라이빗 서브넷 라우팅 테이블을 재구성합니다.

방화벽 자체에는 세 가지 인터페이스가 있습니다.

1. 신뢰할 수 있는 인터페이스: 처리할 트래픽을 수신하기 위한 프라이빗 인터페이스입니다.
2. 신뢰할 수 없는 인터페이스: 트래픽을 인터넷으로 전송하는 퍼블릭 인터페이스입니다. 방화벽은 NAT를 수행하기 때문에 외부 서버는 이러한 퍼블릭 IP 주소의 요청을 수락합니다.
3. 관리 인터페이스: 방화벽 API, 업데이트, 콘솔 등을 위한 프라이빗 인터페이스입니다.

모든 라우팅에서 트래픽은 동일한 가용 영역(AZ) 내에서 유지되어 교차 AZ 트래픽을 줄입니다. 트래픽은 장애 조치가 발생할 때만 AZs를 통과합니다.

허용 목록 수정

온보딩 후 라는 기본 허용 목록이 생성 `ams-allowlist`되며, 여기에는 AMS에 필요한 퍼블릭 엔드포인트와 Windows 및 Linux 호스트 패치를 위한 퍼블릭 엔드포인트가 포함됩니다. 작동하면 AMS 콘솔의 관리 | 관리형 방화벽 | 아웃바운드(Palo Alto) 범주에서 RFC를 생성하여 허용 목록을 생성 또는 삭제하거나 도메인을 수정할 수 있습니다. 는 수정할 수 `ams-allowlist` 없습니다. RFC는 완전 자동으로 처리됩니다(수동이 아님).

사용자 지정 보안 정책

보안 정책은 소스 및 대상 보안 영역, 소스 및 대상 IP 주소, 서비스와 같은 트래픽 속성을 기반으로 세션을 차단할지 또는 허용할지 여부를 결정합니다. 사용자 지정 보안 정책은 완전 자동화된 RFCs에서 지원됩니다. 보안 정책을 생성하거나 삭제할 CTs는 관리 | 관리형 방화벽 | 아웃바운드(Palo Alto) 범주에서 찾을 수 있으며, 기존 보안 정책을 편집할 CT는 배포 | 관리형 방화벽 | 아웃바운드(Palo Alto) 범주에서 찾을 수 있습니다. 새 보안 정책을 생성하거나, 보안 정책을 수정하거나, 보안 정책을 삭제할 수 있습니다.

Note

기본 보안 정책은 수정할 수 `ams-allowlist` 없습니다.

CloudWatch PA 송신 대시보드

CloudWatch에서 두 개의 대시보드를 찾아 Palo Alto(PA)의 집계 보기를 제공할 수 있습니다. AMS-MF-PA-Egress-Config-Dashboard는 PA 구성 개요, 허용 목록 링크, 속성을 포함한 모든 보안 정책 목록을 제공합니다. AMS-MF-PA-Egress-Dashboard를 사용자 지정하여 트래픽 로그를 필터링할 수 있습니다. 예를 들어 보안 정책에 대한 대시보드를 생성하려면 다음과 같은 필터를 사용하여 RFC를 생성할 수 있습니다.

[illegible]

장애 조치 모델

방화벽 솔루션에는 23개의 Palo Alto(PA) 호스트(AZ당 하나)가 포함되어 있습니다. 정상 확인 카나리 아는 일정한 일정에 따라 실행되어 호스트의 상태를 평가합니다. 호스트가 비정상으로 식별되면 AMS 에 알림이 전송되고 라우팅 테이블 변경을 통해 해당 AZ의 트래픽이 다른 AZ의 정상 호스트로 자동으 로 이동합니다. 상태 확인 워크플로가 지속적으로 실행되므로 일시적인 문제 또는 수동 수정으로 인해 호스트가 다시 정상 상태가 되면 정상 호스트를 통해 트래픽이 올바른 AZ로 다시 이동합니다.

확장

AMS는 방화벽의 처리량 및 조정 한도를 모니터링합니다. 처리량 제한이 더 낮은 워터마크 임계값 (CPU/네트워크)을 초과하면 AMS가 알림을 수신합니다. 워터메이커 임계값이 낮으면 리소스가 포화 상태에 도달하여 AMS가 시간 경과에 따른 지표를 평가하고 조정 솔루션을 제안하기 위해에 도달하고 있음을 나타냅니다.

백업 및 복원

백업은 초기 시작 중, 구성 변경 후, 정기적으로 생성됩니다. 초기 시작 백업은 호스트별로 생성되지만 백업 워크플로가 호출될 때 모든 방화벽 호스트에서 구성 변경 및 정기적인 간격 백업이 수행됩니다. AMS 엔지니어는 이러한 기간 외부에서 추가 백업을 생성하거나 요청 시 백업 세부 정보를 제공할 수 있습니다.

AMS 엔지니어는 필요한 경우 구성 백업 복원을 수행할 수 있습니다. 복원이 필요한 경우 모든 호스트에서 복원이 발생하여 호스트 간의 구성을 동기화된 상태로 유지합니다.

복원은 호스트에 인스턴스의 완전한 재할용이 필요한 경우에도 발생할 수 있습니다. 새 EC2 인스턴스가 프로비저닝되면 최신 백업의 자동 복원이 발생합니다. 일반적으로 호스트는 정기적으로 재할용되지 않으며 심각한 장애 또는 필요한 AMI 스왑용으로 예약됩니다. 호스트 휴지통은 수동으로 시작되며 휴지통이 발생하기 전에 알림을 받습니다.

방화벽 구성 백업 외에 특정 허용 목록 규칙은 별도로 백업됩니다. 정의된 허용 목록 규칙이 수정되면 백업이 자동으로 생성됩니다. 필요한 경우 AMS 엔지니어가 허용 목록 백업을 복원할 수 있습니다.

업데이트

AMS Managed Firewall Solution은 시간 경과에 따른 다양한 업데이트가 필요하므로 시스템 개선 사항, 추가 기능 또는 방화벽 운영 체제(OS) 또는 소프트웨어 업데이트를 추가할 수 있습니다.

대부분의 변경 사항은 자동화 인프라 업데이트와 같은 실행 환경에 영향을 미치지 않지만 방화벽 인스턴스 교체 또는 OS 업데이트와 같은 다른 변경 사항으로 인해 중단이 발생할 수 있습니다. 업데이트로 인한 잠재적 서비스 중단이 평가되면 AMS는 유지 관리 기간을 수용하기 위해 사용자와 협력합니다.

운영자 액세스

AMS 운영자는 ActiveDirectory 자격 증명을 사용하여 Palo Alto 디바이스에 로그인하여 작업(예: 패치 적용, 이벤트 응답 등)을 수행합니다. 이 솔루션은 표준 AMS 운영자 인증 및 구성 변경 로그를 유지하여 Palo Alto 호스트에서 수행된 작업을 추적합니다.

기본 로그

기본적으로 방화벽에서 생성된 로그는 각 방화벽의 로컬 스토리지에 있습니다. 초과 근무 시 로컬 로그는 스토리지 사용률에 따라 삭제됩니다. AMS 솔루션은 시스템에서 CloudWatch 로그로 로그를 실시간으로 전송합니다. 자세한 내용은 섹션을 참조하세요 [CloudWatch Logs 통합](#).

AMS 엔지니어는 필요한 경우 시스템에서 직접 로그를 쿼리하고 내보낼 수 있습니다. 또한 로그를 고객 소유 Panorama로 전송할 수 있습니다. 자세한 내용은 섹션을 참조하세요 [Panorama 통합](#).

솔루션에서 수집하는 로그는 다음과 같습니다.

RFC 상태 코드

로그 유형	설명
트래픽	각 세션의 시작 및 종료에 대한 항목을 표시합니다. 각 항목에는 날짜 및 시간, 소스 및 대상 영역, 주소 및 포트, 애플리케이션 이름, 흐름에 적용된 보안 규칙 이름, 규칙 작업(허용, 거부 또는 삭제), 수신 및 송신 인터페이스, 바이트 수 및 세션 종료 이유가 포함됩니다.

로그 유형	설명
	유형 열은 항목이 세션의 시작 또는 종료를 위한 것인지 또는 세션이 거부 또는 삭제되었는지 여부를 나타냅니다. "삭제"는 "모든" 애플리케이션을 지정한 트래픽을 차단한 보안 규칙을 나타내고, "거부"는 규칙이 특정 애플리케이션을 식별했음을 나타냅니다. 규칙이 특정 서비스에 대한 모든 트래픽을 삭제하는 경우와 같이 애플리케이션이 식별되기 전에 트래픽이 삭제되면 애플리케이션은 "해당 없음"으로 표시됩니다.
위협	방화벽에서 생성된 각 보안 경고에 대한 항목을 표시합니다. 각 항목에는 날짜 및 시간, 위협 이름 또는 URL, 소스 및 대상 영역, 주소 및 포트, 애플리케이션 이름, 경고 작업(허용 또는 차단) 및 심각도가 포함됩니다. 유형 열은 "바이러스" 또는 "스파이웨어"와 같은 위협 유형을 나타내고, 이름 열은 위협 설명 또는 URL이며, 범주 열은 위협 범주(예: "키로거") 또는 URL 범주입니다.
URL 필터링	웹 사이트에 대한 액세스와 사용자가 웹 사이트에 자격 증명을 제출할 수 있는지 여부를 제어하는 URL 필터에 대한 로그를 표시합니다.
Configuration	각 구성 변경에 대한 항목을 표시합니다. 각 항목에는 날짜 및 시간, 관리자 사용자 이름, 변경한 IP 주소, 클라이언트 유형(웹 인터페이스 또는 CLI), 명령 실행 유형, 명령 성공 또는 실패 여부, 구성 경로, 변경 전후 값이 포함됩니다.
시스템	각 시스템 이벤트에 대한 항목을 표시합니다. 각 항목에는 날짜 및 시간, 이벤트 심각도, 이벤트 설명이 포함됩니다.
경보	경보 로그는 시스템에서 생성된 경보에 대한 세부 정보를 기록합니다. 이 로그의 정보는 경보에도 보고됩니다. "경보 설정 정의"를 참조하세요.

로그 유형	설명
인증	최종 사용자가 인증 정책 규칙에 의해 액세스가 제어되는 네트워크 리소스에 액세스하려고 할 때 발생하는 인증 이벤트에 대한 정보를 표시합니다. 사용자는이 정보를 사용하여 액세스 문제를 해결하고 필요에 따라 사용자 인증 정책을 조정할 수 있습니다. 상관관계 객체와 함께 사용자는 인증 로그를 사용하여 무차별 대입 공격과 같은 사용자 네트워크에서의 의심스러운 활동을 식별할 수도 있습니다. 선택적으로 사용자는 인증 제한 시간을 로깅하도록 인증 규칙을 구성할 수 있습니다. 이러한 제한 시간은 사용자가 리소스에 대해 한 번만 인증해야 하지만 반복적으로 액세스할 수 있는 기간과 관련이 있습니다. 제한 시간에 대한 정보를 보면 사용자가 제한 시간을 조정할지 여부와 조정 방법을 결정하는 데 도움이 됩니다.
통합	최신 트래픽, 위협, URL 필터링, WildFire 제출 및 데이터 필터링 로그 항목을 단일 보기로 표시합니다. 집합 로그 보기를 사용하면 사용자가 이러한 다양한 유형의 로그를 함께 조사하고 필터링할 수 있습니다(각 로그 세트를 별도로 검색하는 대신). 또는 사용자는 표시할 로그 유형을 선택할 수 있습니다. 필터 필드 왼쪽에 있는 화살표를 클릭하고 트래픽, 위협, URL, 데이터 및/또는 산불을 선택하여 선택한 로그 유형만 표시할 수 있습니다.

이벤트 관리

AMS는 방화벽의 용량, 상태 및 가용성을 지속적으로 모니터링합니다. 방화벽에서 생성된 지표와 AWS/AMS에서 생성된 지표는 문제를 조사하고 해결할 AMS 운영 엔지니어가 수신하는 경보를 생성하는 데 사용됩니다. 현재 경보는 다음과 같은 경우를 다룹니다.

이벤트 경보:

- Firewall Dataplane CPU 사용률
 - CPU 사용률 - Dataplane CPU(트래픽 처리)
- Firewall Dataplane 패킷 사용률이 80% 초과
 - 패킷 사용률 - Dataplane(트래픽 처리)
- Firewall Dataplane 세션 사용률
- 방화벽 Dataplane 세션 활성

- 방화벽 CPU 사용률 집계
 - 모든 CPU/CPUs 사용률
- AZ별 장애 조치
 - AZ에서 장애 조치가 발생할 때 경고 발생
- 비정상 Syslog 호스트
 - Syslog 호스트 상태 확인 실패

관리 경고:

- 상태 확인 모니터 실패 경고
 - 상태 확인 워크플로가 예기치 않게 실패하는 경우
 - 이는 방화벽 상태 확인이 실패하는 경우가 아니라 워크플로 자체를 위한 것입니다.
- 암호 교체 실패 경고
 - 암호 교체에 실패하는 경우
 - API/서비스 사용자 암호는 90일마다 교체됩니다.

지표

모든 지표는 캡처되어 네트워킹 계정의 CloudWatch에 저장됩니다. 이는 네트워킹 계정에 대한 콘솔 액세스 권한을 얻고 CloudWatch 콘솔로 이동하여 볼 수 있습니다. 개별 지표는 지표 탭 또는 선택한 지표의 단일 창 대시보드 보기에서 볼 수 있으며, 집계된 지표는 대시보드 탭으로 이동하여 AMS-MF-PA-Egress-Dashboard를 선택하여 볼 수 있습니다.

사용자 지정 지표:

- 상태 확인
 - 네임스페이스: AMS/MF/PA/Egress
 - PARouteTableConnectionsByAZ
 - PAUnhealthyByInstance
 - PAUnhealthyAggregatedByAZ
 - PAHealthCheckLockState
- 방화벽 생성됨
 - 네임스페이스: AMS/MF/PA/Egress/<instance-id>
 - DataPlaneCPUUtilizationPct

- DataPlanePacketBufferUtilization
- panGPGatewayUtilizationPct
- panSessionActive
- panSessionUtilization

CloudWatch Logs 통합

CloudWatch Logs 통합은 방화벽의 로그를 CloudWatch Logs로 전달하여 로컬 스토리지 사용률로 인한 로그 손실 위험을 완화합니다. 로그는 방화벽이 로그를 생성할 때 실시간으로 채워지며 콘솔 또는 API를 통해 온디맨드로 볼 수 있습니다.

복잡한 쿼리는 로그 분석을 위해 빌드하거나 CloudWatch Insights를 사용하여 CSV로 내보낼 수 있습니다. 또한 사용자 지정 AMS Managed Firewall CloudWatch 대시보드에는 특정 트래픽 로그 쿼리에 대한 빠른 보기와 시간 경과에 따른 트래픽 및 정책 적중률에 대한 그래프 시각화도 표시됩니다. CloudWatch 로그를 사용하면 AWS Kinesis와 같은 다른 AWS 서비스에 대한 기본 통합도 가능합니다.

Note

PA 로그는 기존 온프레미스 또는 타사 Syslog 수집기로 직접 전달할 수 없습니다. AMS Managed Firewall 솔루션은 PA 시스템의 로그를 AWS CloudWatch Logs로 실시간으로 발송합니다. CloudWatch Logs Insight 기능을 사용하여 임시 쿼리를 실행할 수 있습니다. 또한 로그를 Palo Alto의 Panorama 관리 솔루션으로 전송할 수 있습니다. CloudWatch 구독 필터를 사용하여 CloudWatch 로그를 다른 대상으로 전달할 수도 있습니다. 다음 단원에서 Panorama에 대해 자세히 알아보십시오. Splunk에 대한 자세한 내용은 [Splunk과 통합을 참조하세요](#).

Panorama 통합

AMS Managed Firewall은 필요에 따라 기존 Panorama와 통합할 수 있습니다. 이렇게 하면 Panorama에서 방화벽 구성을 보거나 방화벽에서 Panorama로 로그를 전달할 수 있습니다. AMS Managed Firewall과의 Panorama 통합은 읽기 전용이며 Panorama의 방화벽에 대한 구성 변경은 허용되지 않습니다. Panorama는 사용자가 완전히 관리하고 구성하며, AMS는 방화벽과 통신하도록 방화벽을 구성하는 것만 책임집니다.

라이선싱

AMS Managed Firewall의 가격은 사용된 라이선스 유형, 시간당 또는 기존 보유 라이선스 사용(BYOL) 및 어플라이언스가 실행되는 인스턴스 크기에 따라 달라집니다. AWS Marketplace를 통해 선호하는 Palo Alto 방화벽의 인스턴스 크기와 라이선스를 주문해야 합니다.

- Marketplace 라이선스: MALZ의 네트워킹 계정에서 VM 시리즈 차세대 방화벽 번들 1의 이용 약관에 동의합니다.
- BYOL 라이선스: MALZ의 네트워킹 계정에서 VM 시리즈 차세대 방화벽(BYOL)의 이용 약관에 동의하고 AMS에 라이선스를 구매한 후 얻은 "BYOL 인증 코드"를 공유합니다.

제한 사항

현재 AMS는 VM-300 시리즈 또는 VM-500 시리즈 방화벽을 지원합니다. 구성은 [AWS EC2 인스턴스의 VM 시리즈 모델](#),

Note

AMS 솔루션은 AZ의 각 PA 인스턴스가 존경하는 AZ에 대한 송신 트래픽을 처리하므로 Active-Active 모드에서 실행됩니다. 따라서 2개의 AZs에서 각 PA 인스턴스는 최대 5Gbps의 송신 트래픽을 처리하고 2개의 AZs에서 전체 10Gbps 처리량을 효과적으로 제공합니다. 각 AZ의 모든 제한에 대해서도 마찬가지입니다. AMS 상태 확인이 실패하면 잘못된 PA가 있는 AZ에서 다른 AZ로 트래픽을 이동하고 인스턴스 교체 중에 용량이 나머지 AZs 제한으로 줄어듭니다.

AMS는 현재 AWS Marketplace에서 사용할 수 있는 다른 Palo Alto 번들을 지원하지 않습니다. 예를 들어 "VM 시리즈 차세대 방화벽 번들 2"를 요청할 수 없습니다. Palo Alto를 사용하는 AMS Managed Firewall 솔루션은 현재 송신 트래픽 필터링 서비스만 제공하므로 고급 VM 시리즈 번들을 사용하면 추가 기능이나 이점이 제공되지 않습니다.

온보딩 요구 사항

- AWS Marketplace에서 Palo Alto의 VM 시리즈 차세대 방화벽 이용 약관을 검토하고 동의해야 합니다.
- 예상 워크로드에 따라 사용할 인스턴스 크기를 확인해야 합니다.
- 다중 계정 랜딩 존 환경 또는 온프레미스의 네트워크와 충돌하지 않는 /24 CIDR 블록을 제공해야 합니다. 송신 VPC와 클래스가 동일해야 합니다(솔루션은 송신 VPC에 /24 VPC 확장을 프로비저닝함).

요금

AMS Managed Firewall 기본 인프라 비용은 Palo Alto 방화벽을 호스팅하는 EC2 인스턴스, 소프트웨어 라이선스 Palo Alto VM 시리즈 라이선스, CloudWatch Integrations의 세 가지 주요 드라이버로 나뉩니다.

다음 요금은 VM-300 시리즈 방화벽을 기반으로 합니다.

- EC2 인스턴스: Palo Alto 방화벽은 2~3개의 EC2 인스턴스로 구성된 고가용성 모델에서 실행되며, 여기서 인스턴스는 예상 워크로드를 기반으로 합니다. 인스턴스 비용은 리전 및 AZs
 - 예: us-east-1, m5.xlarge, 3AZs
 - $\$0.192 * 24 * 30 * 3 = \$414.72$
 - <https://aws.amazon.com/ec2/pricing/on-demand/>
- Palo Alto 라이선스: Palo Alto VM-300 차세대 방화벽의 소프트웨어 라이선스 비용은 AZ 수와 인스턴스 유형에 따라 달라집니다.
 - 예: us-east-1, m5.xlarge, 3AZs
 - $\$0.87 * 24 * 30 * 3 = \$1879.20$
 - https://aws.amazon.com/marketplace/pp/B083M7JPKB?ref_=srh_res_product_title#pdp-pricing
- CloudWatch Logs 통합: CloudWatch Logs 통합은 SysLog 서버(EC2 - t3.medium), NLB 및 CloudWatch Logs를 활용합니다. 서버 비용은 리전 및 AZs 수를 기준으로 하며, NLB/CloudWatch 로그 비용은 트래픽 사용률에 따라 달라집니다.
 - 예: us-east-1, t3.medium, 3AZ
 - $\$0.0416 * 24 * 30 * 3 = \$89.86$
 - <https://aws.amazon.com/ec2/pricing/on-demand/>
 - <https://aws.amazon.com/cloudwatch/pricing/>

경계(DMZ) VPC

경계 또는 DMZ, VPC에는 AMS 운영 엔지니어가 AMS 네트워크에 액세스하는 데 필요한 리소스가 포함되어 있습니다. 여기에는 2~3AZs에 대한 퍼블릭 서브넷이 포함되어 있으며, AMS Operations 엔지니어가 로그인하거나 터널링할 수 있도록 Auto Scaling 그룹(ASG)에 SSH Bastions 호스트가 있습니다. DMZ 접속에 연결된 보안 그룹에는 Amazon Corp Networks의 포트 22 인바운드 규칙이 포함되어 있습니다.

DMZ VPC CIDR 범위: VPC를 생성할 때 Classless Inter-Domain Routing(CIDR) 블록의 형태로 VPC에 대한 IPv4 주소 범위를 지정해야 합니다. 예: 10.0.16.0/24. 이것은 VPC의 기본 CIDR 블록입니다.

Note

AMS 팀은 향후 방화벽과 같은 다른 리소스가 배포될 경우를 대비하여 버퍼를 제공하기 위해 24(IP 주소가 더 많음)의 범위를 권장합니다.

AWS Transit Gateway

AWS Transit Gateway(TGW)는 Amazon Virtual Private Cloud(VPCs)와 온프레미스 네트워크를 단일 게이트웨이에 연결할 수 있는 서비스입니다. 전송 게이트웨이는 AMS 계정 네트워크와 외부 네트워크 간의 라우팅을 처리하는 네트워킹 백본입니다. 전송 게이트웨이에 대한 자세한 내용은 [AWS Transit Gateway](#)를 참조하세요.

다음 입력을 제공하여 이 리소스를 생성합니다.

- 전송 게이트웨이 ASN 번호*: 전송 게이트웨이의 프라이빗 ASN(자율 시스템 번호)을 제공합니다. 이 ASN은 BGP(Border Gateway Protocol) 세션의 AWS 측에 대한 ASN이어야 합니다. 16비트 ASN의 경우 범위는 64512~65534입니다.

공유 서비스 계정

공유 서비스 계정은 대부분의 AMS 데이터 영역 서비스의 중앙 허브 역할을 합니다. 계정에는 액세스 관리(AD), 엔드포인트 보안 관리(Trend Micro)에 필요한 인프라와 리소스가 포함되어 있으며, 여기에는 고객 접속(SSH/RDP)이 포함되어 있습니다. 공유 서비스 계정에 포함된 리소스에 대한 전반적인 개요는 다음 그림에 나와 있습니다.

공유 서비스 VPC는 세 개의 가용 영역(AZs)에 있는 AD 서브넷, EPS 서브넷 및 고객 접속 서브넷으로 구성됩니다. 공유 서비스 VPC에서 생성된 리소스는 아래에 나열되어 있으며 입력이 필요합니다.

- 공유 서비스 VPC CIDR 범위: VPC를 생성할 때 Classless Inter-Domain Routing(CIDR) 블록의 형태로 VPC에 대한 IPv4 주소 범위를 지정해야 합니다. 예: 10.0.1.0/24. 이것은 VPC의 기본 CIDR 블록입니다.

Note

AMS 팀은 /23의 범위를 권장합니다.

- Active Directory 세부 정보: Microsoft Active Directory(AD)는 모든 AMS 다중 계정 랜딩 존 계정에서 사용자/리소스 관리, 인증/권한 부여 및 DNS에 사용됩니다. 또한 AMS AD는 신뢰 기반 인증을 위해 Active Directory에 대한 단방향 신뢰로 구성됩니다. AD를 생성하려면 다음 입력이 필요합니다.
- Domain Fully Qualified Domain Name(FQDN): AWS Managed Microsoft AD 디렉터리의 정규화된 도메인 이름입니다. 도메인은 네트워크에 있는 기존 도메인 또는 기존 도메인의 하위 도메인이 아니어야 합니다.
- 도메인 NetBIOS 이름: NetBIOS 이름을 지정하지 않으면 AMS는 디렉터리 DNS의 첫 번째 부분으로 이름을 기본 설정합니다. 예를 들어 DNS corp.example.com 디렉터리에 대한 corp입니다.
- Trend Micro - 엔드포인트 보호 보안(EPS): Trend Micro 엔드포인트 보호(EPS)는 운영 체제 보안을 위한 AMS 내의 기본 구성 요소입니다. 시스템은 Deep Security Manager(DSM), EC2 인스턴스, 릴레이 EC2 인스턴스, 모든 데이터 영역 및 고객 EC2 인스턴스 내에 있는 에이전트로 구성됩니다.

공유 서비스 계정EPSMarketplaceSubscriptionRole에서를 수임하고 Trend Micro Deep Security(BYOL) AMI 또는 Trend Micro Deep Security(Marketplace)를 구독해야 합니다.

EPS를 생성하려면 다음 기본 입력이 필요합니다(기본값에서 변경하려는 경우).

- 릴레이 인스턴스 유형: 기본값 - m5.large
- SQL 인스턴스 유형: 기본값 - m5.xlarge
- DB 인스턴스 크기: 기본값 - 200GB
- RDS 인스턴스 유형: 기본값 - db.m5.large
- 고객 접속: AMS 환경의 다른 호스트에 액세스할 수 있도록 공유 서비스 계정에서 SSH 또는 RDP 접속(또는 둘 다)이 제공됩니다. 사용자로서 AMS 네트워크(SSH/RDP)에 액세스하려면 "customer" Bastions를 진입점으로 사용해야 합니다. 네트워크 경로는 온프레미스 네트워크에서 시작되어 DX/VPN을 통해 전송 게이트웨이(TGW)로 이동한 다음 공유 서비스 VPC로 라우팅됩니다. 접속에 액세스할 수 있게 되면 액세스 요청이 부여된 경우 AMS 환경의 다른 호스트로 이동할 수 있습니다.
- SSH 접속에는 다음 입력이 필요합니다.
 - SSH 접속 원하는 인스턴스 용량: 기본값 - 2.
 - SSH 접속 최대 인스턴스: 기본값 - 4.
 - SSH 접속 최소 인스턴스: 기본값 - 2.
 - SSH 접속 인스턴스 유형: 기본값 - m5.large(비용 절감을 위해 변경할 수 있음. 예: t3.medium).
 - SSH 접속 수신 CIDRs: 네트워크의 사용자가 SSH 접속에 액세스하는 IP 주소 범위입니다.

• Windows RDP 접속에는 다음 입력이 필요합니다.

- RDP 접속 인스턴스 유형: 기본값 - t3.medium.
- RDP 접속 원하는 최소 세션: 기본값 - 2.
- RDP 최대 세션: 기본값 - 10.
- RDP 접속 구성 유형: 아래 구성 중 하나를 선택할 수 있습니다.
 - SecureStandard = 사용자가 하나의 Bastion을 수신하고 한 명의 사용자만 Bastion에 연결할 수 있습니다.
 - SecureHA = 사용자가 서로 다른 두 AZ에서 두 개의 Bastion을 수신하여 연결하고 한 명의 사용자만 Bastion에 연결할 수 있습니다.
 - SharedStandard = 한 사용자는 하나의 접속을 수신하여 연결하고 두 사용자는 한 번에 동일한 접속에 연결할 수 있습니다.
 - SharedHA = 한 사용자가 서로 다른 두 AZ에서 두 개의 접속을 수신하여 연결할 수 있고 두 사용자가 한 번에 동일한 접속에 연결할 수 있습니다.
- 고객 RDP 수신 CIDRs: 네트워크의 사용자가 RDP Bastions에 액세스할 IP 주소 범위입니다.

공유 서비스 업데이트: 다중 계정 랜딩 존

AMS는 데이터 영역 릴리스를 사전 통지 없이 매월 관리형 계정에 적용합니다.

AMS는 코어 OU를 사용하여 다중 계정 랜딩 존의 액세스, 네트워킹, EPS, 로그 스토리지, 알림 집계와 같은 공유 서비스를 제공합니다. AMS는 이러한 공유 서비스의 취약성, 패치 및 배포를 해결할 책임이 있습니다. AMS는 사용자가 최신 기능 및 보안 업데이트에 액세스할 수 있도록 이러한 공유 서비스를 제공하는 데 사용되는 리소스를 정기적으로 업데이트합니다. 업데이트는 일반적으로 매월 이루어집니다. 이러한 업데이트의 일부인 리소스는 다음과 같습니다.

- 코어 OU의 일부인 계정입니다.

관리 계정, 공유 서비스 계정, 네트워크 계정, 보안 계정 및 로그 아카이브 계정에는 일반적으로 매월 업데이트되는 RDP 및 SSH 접속, 프록시, 관리 호스트 및 엔드포인트 보안(EPS)에 대한 리소스가 있습니다. AMS는 변경 불가능한 EC2 배포를 공유 서비스 인프라의 일부로 사용합니다.

- 최신 업데이트를 통합하는 새로운 AMS AMIs.

Note

AMS 연산자는 데이터 영역 변경을 실행할 때 내부 경보 억제 변경 유형(CT)을 활용하며 해당 CT의 RFC는 RFC 목록에 표시됩니다. 이는 데이터 플레인 릴리스가 배포될 때 다양한 인프라

가 종료, 재부팅, 오프라인으로 전환되거나 데이터 플레인 배포 중에 불필요한 경보를 트리거하는 배포의 CPU 급증 또는 기타 영향이 있을 수 있기 때문입니다. 배포가 완료되면 모든 인프라가 제대로 실행되고 있는지 확인하고 경보를 다시 활성화합니다.

로그 아카이브 계정

로그 아카이브 계정은 AMS 다중 계정 랜딩 존 환경에서 로그를 보관하기 위한 중앙 허브 역할을 합니다. 계정에는 각 AMS 다중 계정 랜딩 존 환경 계정의 AWS CloudTrail 및 AWS Config 로그 파일 사본이 포함된 S3 버킷이 있습니다. 이 계정을 AWS Firehose 또는 Splunk 등과 함께 중앙 집중식 로깅 솔루션에 사용할 수 있습니다. 이 계정에 대한 AMS 액세스는 몇 명의 사용자로 제한되며, 계정 활동과 관련된 규정 준수 및 포렌식 조사를 위해 감사자 및 보안 팀으로 제한됩니다.

보안 계정

보안 계정은 보안 관련 작업을 수용하기 위한 중앙 허브이자 AMS 컨트롤 플레인 서비스에 알림 및 알림을 퍼널링하기 위한 주요 지점입니다. 또한 보안 계정에는 Amazon Guard Duty 관리 계정과 AWS Config 애그리게이터가 있습니다.

애플리케이션 계정 유형

애플리케이션 계정은 워크로드를 호스팅하는 데 사용하는 AMS 관리형 랜딩 존 아키텍처 내의 AWS 계정입니다. AMS는 세 가지 유형의 애플리케이션 계정을 제공합니다.

- [AMS 관리형 애플리케이션 계정](#)
- [AMS Accelerate 계정](#)
- [고객 관리형 애플리케이션 계정](#)

애플리케이션 계정은 애플리케이션 계정 유형에 따라 AWS Organizations의 다양한 OUs로 그룹화됩니다.

- 루트 OU:
 1. 애플리케이션 OU
 - 관리형 OU: AMS 관리형 계정
 - 개발 OU: 개발자 모드가 활성화된 AMS 관리형 계정

2. OU 가속화: AMS Accelerate 애플리케이션 계정
3. 고객 관리형 OU: 고객 관리형 애플리케이션 계정

애플리케이션 계정은 관리 계정에서 제출된 RFC를 통해 프로비저닝됩니다.

- VPC [ct-1zdasmc2ewzrs](#)를 사용하여 애플리케이션 계정 생성
- Accelerate 계정 생성 [ct-2p93tyd5angmi](#)
- 고객 관리형 애플리케이션 계정 생성 [ct-3pwbixz27n3tn](#)

AMS 관리형 애플리케이션 계정

AMS에서 완전히 관리하는 애플리케이션 계정을 AMS 관리형 애플리케이션 계정이라고 하며, 서비스 요청 관리, 인시던트 관리, 보안 관리, 연속성 관리(백업), 패치 관리, 비용 최적화 또는 인프라의 모니터링 및 이벤트 관리와 같은 일부 또는 모든 운영 작업이 AMS에서 수행됩니다.

AMS에서 수행하는 작업의 양은 선택한 변경 관리 모드에 따라 달라집니다. AMS 관리형 계정은 다양한 변경 관리 모드를 지원합니다.

- [RFC 모드](#)
- [AMS의 직접 변경 모드](#)
- [AMS 및 AWS Service Catalog](#)
- [AMS 고급 개발자 모드](#)
- [AMS의 셀프 서비스 프로비저닝 모드](#)

변경 관리 및 다양한 모드에 대한 자세한 내용은 섹션을 참조하세요 [변경 관리 모드](#).

AMS 관리 없이 AMS 관리형 계정에서 사용할 수 있는 몇 가지 AWS 서비스가 있습니다. 이러한 AWS 서비스의 목록과 이를 AMS 계정에 추가하는 방법은 [셀프 서비스 프로비저닝](#) 섹션에 설명되어 있습니다.

AMS Accelerate 계정

AMS Accelerate는 워크로드를 지원하는 AWS 인프라를 운영할 수 있는 AMS 운영 계획입니다. 새로운 마이그레이션, 가동 중지 시간 경험 또는 AWS 사용 방법 변경 없이 모니터링 및 알림, 인시던트 관리, 보안 관리, 백업 관리와 같은 AMS Accelerate 운영 서비스의 이점을 누릴 수 있습니다. 또한 AMS Accelerate는 정기적인 패치가 필요한 EC2 기반 워크로드에 대한 선택적 패치 추가 기능을 제공합니다.

AMS Accelerate를 사용하면 모든 AWS 서비스를 기본적으로 또는 원하는 도구를 사용하여 사용, 구성 및 배포할 수 있습니다. 선호하는 액세스 및 변경 메커니즘을 사용하는 반면 AMS는 팀을 확장하고, 비용을 최적화하고, 보안 및 효율성을 높이고, 복원력을 개선하는 데 도움이 되는 검증된 사례를 일관되게 적용합니다.

Note

AMS Advanced의 AMS Accelerate 계정에는 AMS 변경 관리(RFCs) 또는 AMS Advanced 콘솔이 없습니다. 대신 AMS Accelerate 콘솔과 기능이 있습니다.

Accelerate 계정은 AMS 다중 계정 랜딩 존 관리 계정에서만 프로비저닝할 수 있습니다. Accelerate는 다양한 운영 기능을 제공합니다. 자세한 내용은 [Accelerate 서비스 설명](#)을 참조하세요.

- 중앙 집중식 로깅, 단일 결제, 보안 계정의 Config Aggregator 및 SCPs.
- AMS Accelerate는 EPS, 액세스 관리, 변경 관리 및 프로비저닝과 같은 일부 AMS 고급 서비스를 제공하지 않습니다. 다음 단계에 따라 액세스 권한을 얻고 전송 게이트웨이(TGW)를 구성하는 것이 좋습니다.

Accelerate에 대한 자세한 내용은 [Accelerate란 무엇입니까?](#)를 참조하십시오.

Accelerate 계정 생성

Accelerate 계정을 생성하려면 [Accelerate 계정 생성에 설명된 단계를 따르세요](#).

Accelerate 계정에 액세스

다중 계정 랜딩 존(MALZ) 계정에서 Accelerate 계정을 프로비저닝한 후 [관리 액세스](#) 권한이 있는 역할인 AccelerateDefaultAdminRole은 사용자가 수임할 계정에 있습니다.

새 Accelerate 계정에 액세스하려면:

1. CustomerDefaultAssumeRole 역할을 사용하여 관리 계정의 IAM 콘솔에 로그인합니다.
2. IAM 콘솔의 탐색 모음에서 사용자 이름을 선택합니다.
3. 역할 전환을 선택합니다. 이 옵션을 처음 선택하면 자세한 정보를 제공하는 페이지가 나타납니다. 그 정보를 읽은 후에 역할 전환(Switch Role)을 클릭합니다. 브라우저 쿠키를 청소하면 이 페이지가 다시 나타나게 할 수 있습니다.
4. 역할 전환 페이지에서 Accelerate 계정 ID와 수임할 역할의 이름을 입력합니다. AccelerateDefaultAdminRole.

이제 액세스 권한이 있으므로 새 IAM 역할을 생성하여 환경에 계속 액세스할 수 있습니다. Accelerate 계정에 SAML 페더레이션을 활용하려면 [SAML 2.0 페더레이션 사용자가 AWS Management Console에 액세스하도록 활성화](#)를 참조하세요.

Transit Gateway에 Accelerate 계정 연결

AMS는 Accelerate 계정의 네트워크 설정을 관리하지 않습니다. AWS APIs를 사용하여 자체 네트워크를 관리하거나([네트워크 솔루션](#) 참조) AMS MALZ에 배포된 기존 Transit Gateway(TGW)를 사용하여 AMS에서 관리하는 MALZ 네트워크에 연결할 수 있습니다.

Note

Accelerate 계정이 동일한 AWS 리전에 있는 경우에만 VPC를 TGW에 연결할 수 있습니다. 자세한 내용은 [전송 게이트웨이를 참조하세요](#).

Accelerate 계정을 Transit Gateway에 추가하려면 [배포 | 관리형 랜딩 존 | 네트워킹 계정 | 정적 경로 추가\(ct-3r2ckznmt0a59\) 변경 유형을 사용하여 새 경로를](#) 요청하고 다음 정보를 포함합니다.

- **블랙홀:** 경로의 대상을 사용할 수 없음을 나타내는 True입니다. Transit Gateway에서 정적 경로의 트래픽을 삭제할 때 작업이 수행됩니다. 트래픽을 지정된 TGW 연결 ID로 라우팅하려면 False입니다. 기본값은 false입니다.
- **DestinationCidrBlock:** 대상 일치에 사용되는 IPV4 CIDR 범위입니다. 라우팅 결정은 가장 구체적인 일치 항목을 기준으로 이루어집니다. 예: 10.0.2.0/24.
- **TransitGatewayAttachmentId:** 라우팅 테이블 대상으로 사용할 TGW 연결 ID입니다. 블랙홀이 false이면이 파라미터가 필요하고, 그렇지 않으면이 파라미터를 비워 둡니다. 예: tgw-attach-04eb40d1e14ec7272.
- **TransitGatewayRouteTableId:** TGW 라우팅 테이블의 ID입니다. 예: tgw-rtb-06ddc751c0c0c881c.

TGW 라우팅 테이블에서 경로를 생성하여이 VPC에 연결합니다.

1. 기본적으로이 VPC는 MALZ 네트워크의 다른 VPCs와 통신할 수 없습니다.
2. 솔루션 아키텍트와 함께이 Accelerate VPCs와 통신할 VPC를 결정합니다.
3. [배포 제출 | 관리형 랜딩 존 | 네트워킹 계정 | 정적 경로\(ct-3r2ckznmt0a59\) 변경 유형을](#) 추가하고 다음 정보를 포함합니다.

- **블랙홀:** 경로의 대상을 사용할 수 없음을 나타내는 True입니다. Transit Gateway에서 정적 경로의 트래픽을 삭제할 때이 작업을 수행합니다. 트래픽을 지정된 TGW 연결 ID로 라우팅하려면 False입니다. 기본값은 false입니다.
- **DestinationCidrBlock:** 대상 일치에 사용되는 IPV4 CIDR 범위입니다. 라우팅 결정은 가장 구체적인 일치 항목을 기준으로 이루어집니다. 예: 10.0.2.0/24.
- **TransitGatewayAttachmentId:** 라우팅 테이블 대상으로 사용할 TGW 연결 ID입니다. 블랙홀이 false인 경우이 파라미터가 필요하며, 그렇지 않으면이 파라미터를 비워 둡니다. 예: tgw-attach-04eb40d1e14ec7272.
- **TransitGatewayRouteTableId:** TGW 라우팅 테이블의 ID입니다. 예: tgw-rtb-06ddc751c0c0c881c.

새 Accelerate 계정 VPC를 AMS 다중 계정 랜딩 존 네트워크에 연결(TGW VPC 연결 생성)

1. 다중 계정 랜딩 존 네트워킹 계정에서 [Amazon VPC 콘솔](#)을 엽니다.
2. 탐색 창에서 Transit Gateway를 선택합니다. 표시되는 전송 게이트웨이의 TGW ID를 기록합니다.
3. Accelerate 계정에서 [Amazon VPC 콘솔](#)을 엽니다.
4. 탐색 창에서 전송 게이트웨이 연결 > 전송 게이트웨이 연결 생성을 선택합니다. 다음과 같이 선택합니다.
 - 전송 게이트웨이 ID에서 2단계에서 기록한 전송 게이트웨이 ID를 선택합니다.
 - 연결 유형(Attachment type)에서 VPC를 선택합니다.
 - 선택적으로 VPC Attachment(VPC 연결)에서 Attachment name tag(연결 이름 태그)에 대한 이름을 입력합니다.
 - DNS 지원 및 IPv6 지원을 활성화할지 선택합니다.
 - VPC ID에서 Transit Gateway에 연결할 VPC를 선택합니다. 이 VPC에는 적어도 하나의 서브넷이 연결되어 있어야 합니다.
 - 서브넷 ID에서 트래픽을 라우팅하기 위해 Transit Gateway에서 사용할 각 가용 영역에 대해 하나의 서브넷을 선택합니다. 하나 이상의 서브넷을 선택해야 합니다. 가용 영역당 서브넷 한 개만 선택할 수 있습니다.
5. 연결 생성(Create attachment)을 선택합니다. 새로 생성된 TGW 연결의 ID를 기록합니다.

TGW 연결을 라우팅 테이블에 연결:

1. VPC를 연결할 TGW 라우팅 테이블을 결정합니다. 배포 | 관리형 랜딩 존 | 네트워킹 계정 | 전송 게이트웨이 라우팅 테이블 생성(ct-3dscwaeyi6cup) 변경 유형을 사용하여 계정 VPCs 가속화를 위한 새 애플리케이션 라우팅 테이블을 생성하는 것이 좋습니다.

2. [관리 제출 | 관리형 랜딩 존 | 네트워킹 계정 | 네트워킹 계정의 TGW 연결\(ct-3nmhh0qr338q6\)](#) RFC를 연결하여 VPC 또는 TGW 연결을 선택한 라우팅 테이블에 연결합니다.

TGW 라우팅 테이블에서 경로를 생성하여이 VPC에 연결합니다.

1. 기본적으로이 VPC는 다중 계정 랜딩 존 네트워크의 다른 VPCs와 통신할 수 없습니다.
2. 솔루션 아키텍트와 함께이 Accelerate 계정 VPCs와 통신할 VPC를 결정합니다.
3. [배포 제출 | 관리형 랜딩 존 | 네트워킹 계정 | 네트워킹 계정에 정적 경로\(ct-3r2ckznmt0a59\)](#) RFC를 [추가하여](#) 필요한 TGW 경로를 생성합니다.

AMS 다중 계정 랜딩 존 전송 게이트웨이를 가리키도록 VPC 라우팅 테이블 구성:

1. 솔루션 아키텍트와 함께 AMS 다중 계정 랜딩 존 전송 게이트웨이로 전송할 트래픽을 결정합니다.
2. [배포 제출 | 관리형 랜딩 존 | 네트워킹 계정 | 네트워킹 계정에 정적 경로\(ct-3r2ckznmt0a59\)](#) RFC를 [추가하여](#) 필요한 TGW 경로를 생성합니다.

고객 관리형 애플리케이션 계정

AMS가 표준 방식으로 관리하지 않는 계정을 생성할 수 있습니다. 이러한 계정을 고객 관리형 계정이라고 하며 AMS에서 관리하는 중앙 집중식 아키텍처의 이점을 활용하면서 계정 내의 인프라를 자체 운영할 수 있는 완전한 제어 기능을 제공합니다.

고객 관리형 계정은 AMS 콘솔 또는 제공하는 서비스(패치, 백업 등)에 액세스할 수 없습니다.

고객 관리형 계정은 AMS 다중 계정 랜딩 존 관리 계정에서만 프로비저닝할 수 있습니다.

다양한 AMS 모드는 애플리케이션 계정에서 다르게 작동합니다. 모드에 대한 자세한 내용은 [AWS Managed Services 모드](#)를 참조하세요.

고객 관리형 애플리케이션 계정을 생성하려면 [관리 계정 | 고객 관리형 애플리케이션 계정 생성](#)을 참조하세요.

고객 관리형 애플리케이션 계정을 삭제하려면 [관리 계정 | 오프보드 애플리케이션 계정](#)을 사용합니다. ([오프보딩 확인](#) CT는 고객 관리형 애플리케이션 계정에 적용되지 않습니다.)

고객 관리형 계정에 액세스

다중 계정 랜딩 존에서 고객 관리형 계정(CMA)을 프로비저닝한 후 (MALZ) 관리자 역할인 CustomerDefaultAdminRole는 SAML 페더레이션을 통해 계정을 구성하기 위해 수입할 계정에 있습니다.

CMA에 액세스하려면:

1. CustomerDefaultAssumeRole 역할을 사용하여 관리 계정의 IAM 콘솔에 로그인합니다.
2. IAM 콘솔의 탐색 모음에서 사용자 이름을 선택합니다.
3. 역할 전환을 선택합니다. 이 옵션을 처음 선택하면 자세한 정보를 제공하는 페이지가 나타납니다. 그 정보를 읽은 후에 역할 전환(Switch Role)을 클릭합니다. 브라우저 쿠키를 청소하면 이 페이지가 다시 나타나게 할 수 있습니다.
4. 역할 전환 페이지에서 고객 관리형 계정 ID와 수입할 역할 이름인 CustomerDefaultAdminRole을 입력합니다.

이제 액세스 권한이 있으므로 새 IAM 역할을 생성하여 환경에 계속 액세스할 수 있습니다. CMA 계정에 SAML 페더레이션을 활용하려면 [SAML 2.0 페더레이션 사용자가 AWS 관리 콘솔에 액세스하도록 활성화](#)를 참조하세요.

Transit Gateway에 CMA 연결

AMS는 고객 관리형 계정(CMAs)의 네트워크 설정을 관리하지 않습니다. AWS APIs 사용하여 자체 네트워크를 관리하거나([네트워크 솔루션](#) 참조) AMS MALZ에 배포된 기존 Transit Gateway(TGW)를 사용하여 AMS에서 관리하는 다중 계정 랜딩 존 네트워크에 연결할 수 있습니다.

Note

CMA가 동일한 AWS 리전에 있는 경우에만 VPC를 TGW에 연결할 수 있습니다. 자세한 내용은 [전송 게이트웨이를 참조하세요](#).

Transit Gateway에 CMA를 추가하려면 [네트워킹 계정 | 정적 경로 추가\(ct-3r2ckznmt0a59\) 변경 유형을 사용하여 새 경로를](#) 요청하고 다음 정보를 포함합니다.

- 블랙홀: 경로의 대상을 사용할 수 없음을 나타내는 True입니다. Transit Gateway에서 정적 경로의 트래픽을 삭제할 때이 작업을 수행합니다. 트래픽을 지정된 TGW 연결 ID로 라우팅하려면 False입니다. 기본값은 false입니다.

- **DestinationCidrBlock**: 대상 일치에 사용되는 IPV4 CIDR 범위입니다. 라우팅 결정은 가장 구체적인 일치 항목을 기준으로 이루어집니다. 예시: 10.0.2.0/24.
- **TransitGatewayAttachmentId**: 라우팅 테이블 대상으로 사용할 TGW 연결 ID입니다. 블랙홀이 false이면이 파라미터가 필요하고, 그렇지 않으면이 파라미터를 비워 둡니다. 예시: tgw-attach-04eb40d1e14ec7272.
- **TransitGatewayRouteTableId**: TGW 라우팅 테이블의 ID입니다. 예시: tgw-rtb-06ddc751c0c0c881c.

AMS 다중 계정 랜딩 존 네트워크에 새 고객 관리형 VPC 연결(TGW VPC 연결 생성):

1. 다중 계정 랜딩 존 네트워킹 계정에서 [Amazon VPC 콘솔](#)을 엽니다.
2. 탐색 창에서 전송 게이트웨이를 선택합니다. 표시되는 전송 게이트웨이의 TGW ID를 기록합니다.
3. 고객 관리형 계정에서 [Amazon VPC 콘솔](#)을 엽니다.
4. 탐색 창에서 전송 게이트웨이 연결 > 전송 게이트웨이 연결 생성을 선택합니다. 다음과 같이 선택합니다.
 - a. 전송 게이트웨이 ID에서 2단계에서 기록한 전송 게이트웨이 ID를 선택합니다.
 - b. 연결 유형(Attachment type)에서 VPC를 선택합니다.
 - c. 선택적으로 VPC Attachment(VPC 연결)에서 Attachment name tag(연결 이름 태그)에 대한 이름을 입력합니다.
 - d. DNS 지원 및 IPv6 지원을 활성화할지 선택합니다.
 - e. VPC ID에서 Transit Gateway에 연결할 VPC를 선택합니다. 이 VPC에는 적어도 하나의 서브넷이 연결되어 있어야 합니다.
 - f. 서브넷 ID에서 트래픽을 라우팅하기 위해 Transit Gateway에서 사용할 각 가용 영역에 대해 하나의 서브넷을 선택합니다. 하나 이상의 서브넷을 선택해야 합니다. 가용 영역당 서브넷 한 개만 선택할 수 있습니다.
5. 연결 생성(Create attachment)을 선택합니다. 새로 생성된 TGW 연결의 ID를 기록합니다.

TGW 연결을 라우팅 테이블에 연결:

VPC를 연결할 TGW 라우팅 테이블을 결정합니다. 배포 | 관리형 랜딩 존 | 네트워킹 계정 | 전송 게이트웨이 라우팅 테이블 생성(ct-3dscwaeyi6cup) RFC를 제출하여 고객 관리형 VPCs에 대한 새 애플리케이션 라우팅 테이블을 생성하는 것이 좋습니다. VPC 또는 TGW 연결을 선택한 라우팅 테이블에 연

결하려면 네트워킹 계정에서 배포 | 관리형 랜딩 존 | 네트워킹 계정 | TGW 연결(ct-3nmhh0qr338q6) RFC를 제출합니다.

TGW 라우팅 테이블에서 경로를 생성하여이 VPC에 연결합니다.

1. 기본적으로이 VPC는 다중 계정 랜딩 존 네트워크의 다른 VPCs와 통신할 수 없습니다.
2. 솔루션 아키텍트와 함께이 고객 관리형 VPCs와 통신할 VPC를 결정합니다. 배포 제출 | 관리형 랜딩 존 | 네트워킹 계정 | 네트워킹 계정에 정적 경로(ct-3r2ckznm0a59) RFC를 추가하여 필요한 TGW 경로를 생성합니다.

Note

이 CT(ct-3r2ckznm0a59)는 코어 라우팅 테이블 EgressRouteDomain에 정적 경로를 추가하는 것을 허용하지 않습니다. CMA가 송신 트래픽을 허용해야 하는 경우 ct-0xdawir96cy7k를 사용하여 관리 | 기타 | 기타(MOO) RFC를 제출합니다.

AMS 다중 계정 랜딩 존 전송 게이트웨이를 가리키도록 VPC 라우팅 테이블 구성:

솔루션 아키텍트와 함께 AMS 다중 계정 랜딩 존 전송 게이트웨이로 전송할 트래픽을 결정합니다. 이전에 생성된 TGW 연결로 트래픽을 전송하도록 VPC 라우팅 테이블 업데이트

고객 관리형 계정에 대한 운영 지원 받기

AMS는 계정을 AMS Accelerate에 온보딩하여 고객 관리형 계정에 배포한 워크로드를 운영하는 데 도움이 될 수 있습니다. AMS Accelerate를 사용하면 새 마이그레이션을 거치거나 가동 중지 시간을 경험하거나 사용 방법을 변경하지 않고도 모니터링 및 알림, 인시던트 관리, 보안 관리, 백업 관리와 같은 운영 서비스의 이점을 누릴 수 있습니다 AWS. 또한 AMS Accelerate는 정기적인 패치가 필요한 EC2-based 워크로드에 대한 선택적 패치 추가 기능을 제공합니다. AMS Accelerate를 사용하면 AMS Advanced Customer Managed 계정과 마찬가지로 모든 AWS 서비스를 기본적으로 또는 원하는 도구를 사용하여 계속 사용, 구성 및 배포할 수 있습니다. 선호하는 액세스 및 변경 메커니즘을 사용하는 반면 AMS는 팀을 확장하고, 비용을 최적화하고, 보안 및 효율성을 높이고, 복원력을 개선하는 데 도움이 되는 검증된 사례를 적용합니다. 자세한 내용은 [Accelerate 서비스 설명](#)을 참조하세요.

Customer Managed 계정을 Accelerate에 온보딩하려면 CSDM에 문의하여 [AMS Accelerate 시작하기](#)의 단계를 따르세요.

Note

AMS Advanced의 AMS Accelerate 계정에는 AMS 변경 관리(변경 요청 또는 RFCs) 또는 AMS Advanced 콘솔이 없습니다. 대신 AMS Accelerate 콘솔과 기능이 있습니다.

AMS 도구 계정(워크로드 마이그레이션)

다중 계정 랜딩 존 도구 계정(VPC 포함)은 마이그레이션 작업을 가속화하고, 보안 위치를 높이고, 비용과 복잡성을 줄이고, 사용 패턴을 표준화하는 데 도움이 됩니다.

도구 계정은 다음을 제공합니다.

- 프로덕션 워크로드 외부의 시스템 통합자를 위한 복제 인스턴스에 액세스하기 위한 잘 정의된 경계입니다.
- 격리된 체임버를 생성하여 다른 워크로드의 계정에 배치하기 전에 워크로드에 맬웨어 또는 알 수 없는 네트워크 경로가 있는지 확인할 수 있습니다.
- 정의된 계정 설정으로서 워크로드 마이그레이션을 위해 온보딩하고 설정하는 데 더 빠른 시간을 제공합니다.
- 격리된 네트워크는 온프레미스 -> CloudEndure -> 도구 계정 -> AMS 수집 이미지에서 트래픽을 보호하기 위해 라우팅됩니다. 이미지가 수집되면 AMS 관리 | 고급 스택 구성 요소 | AMI | 공유 (ct-1eiczxw8ihc18) RFC를 통해 대상 계정과 이미지를 공유할 수 있습니다.

상위 수준 아키텍처 다이어그램:

배포 | 관리형 랜딩 존 | 관리 계정 | 도구 계정 생성(VPC 사용) 변경 유형(ct-2j7q1hgf26x5c)을 사용하여 다중 계정 랜딩 존 환경 내에서 도구 계정을 빠르게 배포하고 워크로드 수집 프로세스를 인스턴스화합니다. [관리 계정, 도구 계정: 생성\(VPC 사용\)을 참조하세요.](#)

Note

마이그레이션 허브이므로 가용 영역(AZs)이 두 개 있는 것이 좋습니다. 기본적으로 AMS는 모든 계정에 다음과 같은 두 개의 보안 그룹(SGs)을 생성합니다. 이 두 SGs 있는지 확인합니다. 없는 경우 AMS 팀과 함께 새 서비스 요청을 열어 요청하세요.

- SentinelDefaultSecurityGroupPrivateOnlyEgressAll
- InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

온프레미스로 돌아가는 경로가 있는 프라이빗 서브넷에서 CloudEndure 복제 인스턴스가 생성되었는지 확인합니다. 프라이빗 서브넷의 라우팅 테이블에 TGW로 돌아가는 기본 라우팅이 있는지 확인하여 확인할 수 있습니다. 그러나 CloudEndure 시스템 전환을 수행하면 온프레미스로 돌아가는 경로가 없는 "격리된" 프라이빗 서브넷으로 이동해야 하며 인터넷 아웃바운드 트래픽만 허용됩니다. 온프레미스 리소스에 대한 잠재적 문제를 방지하려면 격리된 서브넷에서 전환이 발생하도록 하는 것이 중요합니다.

사전 조건:

1. Plus 또는 Premium 지원 수준.
2. AMIs IDs입니다.
3. 앞서 설명한 대로 생성된 도구 계정입니다.

AWS Application Migration Service(AWS MGN)

AWS MGN([AWS Application Migration Service](#))은 도구 계정 프로비저닝 중에 자동으로 생성되는 `AWSManagedServicesMigrationRole` IAM 역할을 통해 MALZ 도구 계정에서 사용할 수 있습니다. AWS MGN을 사용하여 지원되는 버전의 Windows 및 Linux [운영 체제에서 실행되는 애플리케이션과 데이터베이스를 마이그레이션할 수 있습니다](#).

AWS 리전 지원에 대한 up-to-date 정보는 [AWS 리전 서비스 목록을 참조하세요](#).

선호하는 AWS 리전 가 현재 AWS MGN에서 지원되지 않거나 애플리케이션이 실행되는 운영 체제가 현재 AWS MGN에서 지원되지 않는 경우 도구 계정에서 [CloudEndure 마이그레이션](#)을 대신 사용하는 것이 좋습니다.

AWS MGN 초기화 요청

AWS MGN은 처음 사용하기 전에 AMS로 [초기화](#)해야 합니다. 새 도구 계정에 대해 이를 요청하려면 도구 계정에서 다음 세부 정보와 함께 관리 | 기타 | 기타 RFC를 제출합니다.

RFC Subject=Please initialize AWS MGN in this account

RFC Comment=Please click 'Get started' on the MGN welcome page here:

https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using all default values to 'Create template' and complete the initialization process.

AMS가 RFC를 성공적으로 완료하고 도구 계정에서 AWS MGN을 초기화하면 AWSManagedServicesMigrationRole를 사용하여 요구 사항에 맞는 기본 템플릿을 편집할 수 있습니다.

새 AMS 도구 계정에 대한 액세스 활성화

도구 계정이 생성되면 AMS는 계정 ID를 제공합니다. 다음 단계는 새 계정에 대한 액세스를 구성하는 것입니다. 단계는 다음과 같습니다.

1. 적절한 Active Directory 그룹을 적절한 계정 IDs.

새 AMS 생성 계정은 사용자가 RFC를 제출할 수 있도록 허용하는 역할뿐만 아니라 ReadOnly 역할 정책으로 프로비저닝됩니다. RFCs

도구 계정에는 다음과 같은 추가 IAM 역할과 사용자가 있습니다.

- IAM 역할: AWSManagedServicesMigrationRole
- IAM 사용자: customer_cloud_endure_user

2. 서비스 통합 팀원이 다음 수준의 도구를 설정할 수 있도록 정책 및 역할을 요청합니다.

AMS 콘솔로 이동하여 다음 RFCs를 제출합니다.

a. KMS 키를 생성합니다. [KMS 키 생성\(자동\)](#) 또는 [KMS 키 생성\(검토 필요\)](#)을 사용합니다.

KMS를 사용하여 수집된 리소스를 암호화할 때 다중 계정 랜딩 존 애플리케이션 계정의 나머지 부분과 공유되는 단일 KMS 키를 사용하면 대상 계정에서 복호화할 수 있는 수집된 이미지에 대한 보안을 제공합니다.

b. KMS 키를 공유합니다.

관리 | 고급 스택 구성 요소 | KMS 키 | 공유(검토 필요) 변경 유형(ct-05yb337abq3x5)을 사용하여 수집된 AMIs가 상주할 애플리케이션 계정과 새 KMS 키를 공유하도록 요청합니다.

최종 계정 설정의 예제 그래픽:

AMS 사전 승인된 IAM CloudEndure 정책 예제

AMS 사전 승인된 IAM CloudEndure 정책을 보려면: [WIGS Cloud Endure Landing Zone 예제](#) 파일의 압축을 풀고 `customer_cloud_endure_policy.json`을 엽니다.

AMS 도구 계정 연결 및 end-to-end 설정 테스트

1. 먼저 CloudEndure를 구성하고 AMS에 복제할 서버에 CloudEndure 에이전트를 설치합니다.
2. CloudEndure에서 프로젝트를 생성합니다.
3. 보안 암호 관리자를 통해 사전 조건을 수행할 때 공유된 AWS 자격 증명을 입력합니다.
4. 복제 설정에서:
 - a. 복제 서버에 적용할 보안 그룹 선택 옵션에서 AMS "Sentinel" 보안 그룹(프라이빗 전용 및 EgressAll)을 모두 선택합니다.
 - b. 시스템(인스턴스)에 대한 전환 옵션을 정의합니다. 자세한 내용은 [5단계를 참조하세요. 컷오버](#)
 - c. 서브넷: 프라이빗 서브넷입니다.
5. 보안 그룹:
 - a. AMS "Sentinel" 보안 그룹(프라이빗 전용 및 EgressAll)을 모두 선택합니다.
 - b. 전환 인스턴스는 AMS 관리형 Active Directory(MAD) 및 AWS 퍼블릭 엔드포인트와 통신해야 합니다.
 - i. 탄력적 IP: 없음
 - ii. 퍼블릭 IP: 아니요
 - iii. IAM 역할: customer-mc-ec2-instance-profile
 - c. 내부 태그 지정 규칙에 따라 태그를 설정합니다.
6. 시스템에 CloudEndure 에이전트를 설치하고 EC2 콘솔의 AMS 계정에 표시될 복제 인스턴스를 찾습니다.

AMS 수집 프로세스:

AMS 도구 계정 위생

계정에서 AMI를 공유했으며 복제된 인스턴스가 더 이상 필요하지 않은 경우 정리해야 합니다.

- 사후 인스턴스 WIGs 수집:
 - 전환 인스턴스: AWS 콘솔을 통해 작업이 완료된 후 최소한이 인스턴스를 중지하거나 종료합니다.
 - 사전 수집 AMI 백업: 인스턴스가 수집되고 온프레미스 인스턴스가 종료되면 제거
 - AMS 수집 인스턴스: AMI가 공유되면 스택을 끄거나 종료합니다.
 - AMS 수집 AMIs: 대상 계정과의 공유가 완료되면 삭제

- 마이그레이션 정리 종료: 정기적으로 정리가 이루어지도록 개발자 모드를 통해 배포된 리소스를 문서화합니다. 예를 들면 다음과 같습니다.
 - 보안 그룹
 - 클라우드 형식을 통해 생성된 리소스
 - 네트워크 ACK
 - 서브넷
 - VPC
 - 라우팅 테이블
 - 역할
 - 사용자 및 계정

대규모 마이그레이션 - Migration Factory

[AWS CloudEndure Migration Factory 솔루션 소개](#)를 참조하세요.

SALZ 네트워크 아키텍처

다음 다이어그램은 AWS Managed Services(AMS) 단일 계정 랜딩 존(SALZ) VPC 네트워크 레이아웃을 나타내며 가용성이 높은 설정의 예입니다.

AMS는 표준 템플릿과 온보딩 중에 제공된 선택한 옵션을 기반으로 네트워킹의 모든 측면을 구성합니다. 표준 AWS 네트워크 설계가 AWS 계정에 적용되고 Virtual Private Cloud(VPC)가 생성되어 VPN 또는 Direct Connect를 통해 AMS에 연결됩니다. AWS Direct Connect에서 [Direct Connect](#)에 대해 자세히 알아보세요. 표준 VPCs에는 DMZ, 공유 서비스 및 애플리케이션 서브넷이 포함됩니다. 온보딩 프로세스 중에 필요에 맞게 추가 VPCs를 요청하고 생성할 수 있습니다(예: 고객 부서, 파트너). 온보딩 후에는 네트워크 다이어그램이 제공됩니다. 환경 문서는 네트워크 설정 방법을 설명합니다.

Note

모든 활성 서비스의 기본 서비스 제한 및 제약 조건에 대한 자세한 내용은 [AWS 서비스 제한 설명서를 참조하세요](#).

네트워크 설계는 Amazon "[최소 권한 원칙](#)"을 기반으로 구축되었습니다. 이를 위해 신뢰할 수 있는 네트워크에서 들어오는 트래픽을 제외한 모든 인바운드 및 아웃바운드 트래픽을 게이트웨이를 통해 라우팅합니다. 유일하게 신뢰할 수 있는 네트워크는 VPN 및/또는 AWS Direct Connect(DX)를 사용하여 온프레미스 환경과 VPC 간에 구성된 네트워크입니다. 접속 인스턴스를 사용하여 액세스 권한이 부여되므로 프로덕션 리소스에 직접 액세스할 수 없습니다. 모든 애플리케이션과 리소스는 퍼블릭 로드 밸런서를 통해 연결할 수 있는 프라이빗 서브넷 내에 있습니다. 퍼블릭 송신 트래픽은 순방향 프록시를 통해 인터넷 게이트웨이로 흐른 다음 인터넷으로 흐릅니다. 또는 트래픽이 VPN 또는 Direct Connect를 통해 온프레미스 환경으로 흐를 수 있습니다.

AMS 단일 계정 랜딩 존 공유 서비스

공유 서비스 서브넷에는 AMS Directory Services, 프로비저닝 및 일반 작업을 자동화하는 관리 호스트, 바이러스 백신(TrendMicro) 관리 서버 및 내부 접속 호스트가 포함됩니다.

- AMS 디렉터리 서비스 = AD 도메인 컨트롤러

AMS 계정에서 Active Directory를 생성하고, AMS 도메인을 생성하고, 시작 시 관리형 스택을 도메인에 조인합니다.

- 관리 호스트 = AMS 관리 호스트(프로비저닝 및 일반 작업 자동화)

API 엔드포인트 역할을 하여 AWS Directory Service 도메인 컨트롤러를 수정 AWS Directory Service하고 상호 작용합니다.

- 보안 서비스: 바이러스 백신(TrendMicro) 관리 서버 = EPS" + EPS 릴레이

Trend Micro™ Deep Security 소프트웨어(DSM)를 활용하고, 클라이언트-서버 모델에서 작동하며, Deep Security 관리자, 에이전트 및 릴레이를 포함하는 백엔드 데이터베이스를 갖추고 있습니다.

- 내부 접속 호스트 = 고객 접속

인터넷의 기본 액세스 포인트가 되고 다른 Amazon EC2 인스턴스에 대한 프록시 역할을 하도록 설계된 특수 목적 서버입니다.

AMS 설정

주제

- [AMS 기본 설정 이해](#)
- [AMS 콘솔 사용](#)
- [AMS API 및 CLI 사용](#)
- [AMS에서 자체 EPS 사용](#)
- [AMS 알림 수신](#)
- [프라이빗 및 퍼블릭 DNS 설정](#)
- [AMS 송신 트래픽 관리](#)
- [AMS Advanced에 IAM 리소스 배포](#)
- [IAM 역할 및 프로파일을 사용하여 AMS에서 권한 설정](#)
- [AD FS 클레임 규칙 및 SAML 설정](#)
- [네트워크 ACL로 제한](#)
- [Outposts의 AMS](#)
- [AMS에서 태그 사용](#)
- [AWS Managed Services 리소스 스케줄러](#)
- [AWS Systems Manager AMS Advanced의](#)
- [AMS 계정 오프보드](#)

온보딩 시 일부 AMS 설정 작업이 완료될 수 있습니다.

AMS를 포함한 역할 및 책임에 대한 전체 설명은 섹션을 [지원되는 AWS 서비스](#) 참조하세요 [AMS 책임 매트릭스\(RACI\)](#).

Note

AMS가 추가 AWS 서비스를 제공하도록 요청하려면 서비스 요청을 제출합니다. 이 요청을 하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [서비스 요청 관리](#).

AMS 기본 설정 이해

AWS Managed Services(AMS) 네트워크에는 대부분의 서비스에 대한 기본값이 포함된 표준화된 구성이 있습니다.

이 섹션에서는 AMS가 액세스, 모니터링 및 로깅, 관리에 사용하는 기본 설정을 설명합니다.

다중 계정 랜딩 존 또는 단일 계정 랜딩 존 인프라 비용의 예는 섹션을 참조하세요 [AMS 환경 기본 구성 요소](#).

주제

- [DNS 확인 기본값\(MALZ\)](#)
- [EC2 IAM 인스턴스 프로파일](#)
- [AMS의 기준 모니터링 알림](#)
- [로그 보존 및 교체 기본값](#)

DNS 확인 기본값(MALZ)

AWS Managed Services(AMS) 다중 계정 랜딩 존: AWS 환경에서는 Resolver 전달 규칙을 구성하여 Route 53 Resolver와 VPC의 DNS 해석기 간의 도메인 이름 시스템(DNS) 확인을 통합할 수 있습니다. DNS 쿼리를 전달하는 데 이러한 규칙을 사용하려면 먼저 이러한 쿼리를 전달할 수 있도록 인바운드 및 아웃바운드 해석기 엔드포인트를 설정해야 합니다.

기본적으로 AMS의 다중 계정 설정에서 애플리케이션 계정 VPCs 내의 DNS 쿼리는 공유 서비스 계정에 있는 Microsoft Active Directory용 AWS Directory Service(Managed AD라고도 함) 도메인의 조건부 전달자에게 전달됩니다. AMS를 사용하면 AmazonProvidedDNS를 사용하여 DNS 쿼리를 전달할 AmazonProvidedDNS 수 있습니다. 이를 통해 현재 Amazon Route 53을 통해 Amazon에서 제공하는 DNS만 지원하는 VPC 엔드포인트를 활용할 수 있습니다. 이에 따라 공유 서비스 계정에 기본적으로 배포되는 공통 VPC 엔드포인트에 대해서도 해석기 규칙이 자동으로 설정됩니다. 이러한 공통 VPC 엔드포인트에 대한 자세한 내용은 섹션을 참조하세요 [AMS VPC 엔드포인트](#).

VPCs에서 DHCP(Dynamic Host Configuration Protocol) 옵션 세트를 구성하려면 및 공유 서비스 계정의 공통 VPC 엔드포인트를 가리키는 Route53 Resolver 규칙이 있음(온프레미스 도메인에 대한 선택적 해석기 규칙 포함), 관리 생성 | 기타 | 기타 | 공유 서비스 계정을 지정하는 변경 요청(RFC) 생성, 및 VPC 엔드포인트에 대한 애플리케이션 계정 VPC 로컬 DNS 및 Route 53 Resolver 규칙의 활성화를 요청합니다.

EC2 IAM 인스턴스 프로파일

인스턴스 프로파일은 IAM 역할을 위한 컨테이너로서 인스턴스 시작 시 EC2 인스턴스에 역할 정보를 전달하는 데 사용할 수 있습니다.

MALZ

AMS 기본 인스턴스 프로파일은 `customer-mc-ec2-instance-profile` 및 `customer-mc-ec2-instance-profile-s3`입니다. 이러한 인스턴스 프로파일은 다음 표에 설명된 권한을 제공합니다.

정책 설명

프로필	정책
customer-mc-ec2-instance-profile	AmazonSSMManagedInstanceCore : Ec2 인스턴스가 SSM 에이전트를 사용하도록 허용합니다.
	AMSInstanceProfileLoggingPolicy : Ec2 인스턴스가 로그를 S3 및 CloudWatch로 푸시하도록 허용합니다.
	AMSInstanceProfileManagementPolicy : Ec2 인스턴스가 Active Directory 조인과 같은 부팅 작업을 수행하도록 허용합니다.
	AMSInstanceProfileMonitoringPolicy : Ec2 인스턴스가 결과를 AMS 모니터링 서비스에 보고할 수 있도록 허용합니다.
	AMSInstanceProfilePatchPolicy : Ec2 인스턴스가 패치를 수신하도록 허용합니다.
customer-mc-ec2-instance-profile-s3	AMSInstanceProfileBYOEPSPolicy : Ec2 인스턴스가 AMS Bring Your Own EPS 를 사용하도록 허용합니다.
	AMSInstanceProfileLoggingPolicy : Ec2 인스턴스가 로그를 S3 및 CloudWatch로 푸시하도록 허용합니다.

프로필	정책
	AMSInstanceProfileManagementPolicy : Ec2 인스턴스가 Active Directory 조인과 같은 부팅 작업을 수행하도록 허용합니다.
	AMSInstanceProfileMonitoringPolicy : Ec2 인스턴스가 결과를 AMS 모니터링 서비스에 보고할 수 있도록 허용합니다.
	AMSInstanceProfilePatchPolicy : Ec2 인스턴스가 패치를 수신하도록 허용합니다.
	AMSInstanceProfileS3WritePolicy : Ec2 인스턴스가 고객 S3 버킷을 읽고 쓸 수 있도록 허용합니다.

SALZ

IAM 인스턴스 정책의 권한을 `customer-mc-ec2-instance-profile` 부여하는 AMS 기본 인스턴스 프로파일 하나 있습니다 `customer_ec2_instance_profile_policy`. 이 인스턴스 프로파일은 다음 표에 설명된 권한을 제공합니다. 프로파일은 인스턴스에 로그인하는 사용자가 아닌 인스턴스에서 실행되는 애플리케이션에 권한을 부여합니다.

정책에는 종종 여러 문이 포함되며, 각 문은 서로 다른 리소스 세트에 권한을 부여하거나 특정 조건에서 권한을 부여합니다.

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).

EC2 기본 IAM 인스턴스 프로파일 권한

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).			
정책 문	Effect	작업	설명 및 리소스(ARN)
Amazon Elastic Compute Cloud(Amazon EC2)			
EC2 메시지 작업	허용	AcknowledgeMessage, DeleteMessage,	계정에서 EC2 Systems Manager 메시징 작업을 허용합니다.

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).

정책 문	Effect	작업	설명 및 리소스(ARN)
		FailMessage, GetEndpoint, GetMessages, SendReply	
Ec2 설명	허용	* (모두)	콘솔이 계정에서 EC2의 구성 세부 정보를 표시하도록 허용합니다.
Iam 역할 ID 가져 오기	허용	GetRole	EC2가 aws:iam::*:role/customer-* 및에서 IAM ID를 가져오도록 허용합니다aws:iam::*:role/customer_*
로그 이벤트를 업로드할 인스턴스	허용	로그 그룹 생성	로그를 생성할 수 있는 위치: aws:logs::*:log-group:i-*
		로그 스트림 생성	로그를 다음으로 스트리밍할 수 있습니다. aws:logs::*:log-group:i-*
MMS용 CW	허용	DescribeAlarms, PutMetricAlarm, PutMetricData	CloudWatch가 계정에서 경보를 검색할 수 있도록 허용합니다. CW가 경보를 생성 또는 업데이트하고 지정된 지표와 연결할 수 있도록 허용합니다. CW가 지표 데이터 포인트를 계정에 게시할 수 있도록 허용합니다.

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).

정책 문	Effect	작업	설명 및 리소스(ARN)
Ec2 태그	허용	CreateTags, DescribeTags,	계정의 지정된 인스턴스에서 태그를 추가, 덮어쓰기 및 설명할 수 있습니다.
CW 로그를 명시적으로 거부	거부	DescribeLogStreams, FilterLogEvents, GetLogEvents	다음에 대한 로그 스트림 나열, 필터링 또는 가져오기를 허용하지 않습니다. <code>aws:logs:*:*:log-group:/mc/*</code>
Amazon EC2 Simple Systems Manager(SSM)			
SSM 작업	허용	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	계정에서 다양한 SSM 함수를 허용합니다.
S3의 SSM 액세스	허용	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadParts, ListBucketMultipartUploads	EC2의 SSM이에서 객체를 가져오고 업데이트하며에 대한 멀티파트 객체 업로드를 중단하고에서 멀티파트 업로드에 사용할 수 있는 포트 및 버킷을 나열할 수 있도록 허용합니다. <code>aws:s3:::mc-*:internal-*/aws/ssm*</code>

Amazon EC2 Simple Storage Service(S3)

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).

정책 문	Effect	작업	설명 및 리소스(ARN)
S3에서 객체 가져 오기	허용	Get List	EC2 애플리케이션이 계정의 S3 버킷에서 객체를 검색하고 나열할 수 있도록 허용합니다.
고객 암호화 로그 S3 액세스	허용	PutObject	EC2 애플리케이션이에서 객체를 업데이트하도록 허용 <code>aws:s3:::mc-*-logs-*/encrypted/app/*</code>
패치 데이터 객체 S3 추가	허용	PutObject	EC2 애플리케이션이에서 S3 버킷에 패치 적용 데이터를 업로드하도록 허용 <code>aws:s3:::awsms-a*-patch-data-*</code>
S3에 자체 로그 업로드	허용	PutObject	EC2 애플리케이션이 사용자 지정 로그를 다음에 업로드하도록 허용합니다. <code>aws:s3:::mc-a*-logs-*/aws/instances/*/\${aws:userid}/*</code>
MC 네임스페이스 S3 로그를 명시적으로 거부	거부	GetObject* Put*	EC2 애플리케이션이 다음과 같이 객체를 가져오거나 배치하는 것을 허용하지 않습니다. <code>aws:s3:::mc-*-logs-*/encrypted/mc*</code> , <code>aws:s3:::mc-*-logs-*/mc/*</code> , <code>aws:s3:::mc-a*-logs-**-audit/*</code>

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).

정책 문	Effect	작업	설명 및 리소스(ARN)
S3 삭제를 명시적으로 거부	거부	* (모두)	EC2 애플리케이션이 다음의 객체에 대해 어떤 작업도 수행하는 것을 허용하지 않습니다. aws:s3:::mc-a*-logs-*/* , aws:s3:::mc-a*-internal-*/* ,
S3 CFN 버킷을 명시적으로 거부	거부	Delete*	다음에서 객체를 삭제하는 EC2 애플리케이션을 허용하지 않습니다. aws:s3:::cf-templates-*
명시적으로 거부 목록 버킷 S3	거부	ListBucket	다음에서 암호화된 객체, 감사 로그 또는 예약된 (mc) 객체를 나열할 수 없습니다. aws:s3:::mc-*-logs-*

AWS Secrets Manager Amazon EC2의

CW = CloudWatch. ARN = Amazon 리소스 이름. * = 와일드카드(임의).

정책 문	Effect	작업	설명 및 리소스(ARN)
Trend Cloud One 보안 암호 액세스	허용	GetSecretValue	Amazon EC2가 Trend Cloud One 마이그레이션을 위한 보안 암호에 액세스할 수 있도록 허용합니다. <pre>aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- id* , arn:aws:secretsman ager:~::~secret:/ams/ eps/cloud-one-agent- activation-token* , aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- id* , aws:secretsmanager :~::~secret:/ams/eps/ cloud-one-agent-tenant- guid*</pre>

AWS Key Management Service Amazon EC2의

Trend Cloud One 복호화 키	허용	Decrypt	Amazon EC2가 별칭 이름 /ams/eps/cloudone-migration으로 AWS KMS 키를 복호화하도록 허용 <pre>arn:aws:kms:~::~alias/ ams/eps/cloudone-migrat ion</pre>

Amazon IAM 정책에 익숙하지 않은 경우 중요 정보는 [IAM 정책 개요](#)를 참조하세요.

Note

정책에는 종종 여러 문이 포함되며, 각 문은 서로 다른 리소스 세트에 권한을 부여하거나 특정 조건에서 권한을 부여합니다.

AMS의 기준 모니터링 알림

AMS 모니터링 기본값에 대해 알아봅니다. 자세한 내용은 [AMS의 모니터링 및 이벤트 관리](#) 단원을 참조하십시오.

다음 표에는 모니터링되는 항목과 기본 알림 임계값이 나와 있습니다. 원하는 변경 사항을 결정하고 관련 CloudWatch Amazon SNS 주제를 구독한 후 관리 | 기타 | 기타 | 업데이트(ct-0xdawir96cy7k) RFC를 사용하여 알림 임계값을 변경할 수 있습니다. 주제 생성 및 구독에 대한 자세한 내용은 [주제 구독을 참조하세요](#). 일반 정보는 [Amazon SNS FAQs](#). 경보가 임계값을 초과할 때 직접 알림을 받으려면 AMS의 표준 알림 프로세스 외에도 경보 구성을 덮어쓰는 방법에 대한 다음 지침을 따르세요 [AMS에서 생성된 알림 수신](#).

Amazon CloudWatch는 지표의 보존 기간을 연장합니다. 자세한 내용은 [CloudWatch 제한을 참조하세요](#).

Note

AMS는 정기적으로 기준 모니터링을 보정합니다. 새 계정은 항상 최신 기준 모니터링으로 온보딩되며 표에는 새로 온보딩된 계정에 대한 기준 모니터링이 설명되어 있습니다. AMS는 기존 계정의 기준 모니터링을 정기적으로 업데이트하며 업데이트가 적용되기 전에 시간 지연이 발생할 수 있습니다. 자세한 내용은 [AMS 계정에 대한 모니터링 구성 보기](#) 단원을 참조하십시오.

Note

EC2 인스턴스 알림Non-root volume usage은 기본적으로 비활성화되어 있습니다. 이 경보를 기반으로 경보를 생성해야 하는 경우 RFC 변경 유형 [ct-0erkoadd6uyvg](#)를 사용하여 경보를 활성화해야 합니다.

기존 모니터링의 알림

서비스:	보안 알림	알림 이름 및 트리거 조건	참고

별표가 지정된(*) 알림의 경우 AMS는 가능한 경우 영향을 사전에 평가하고 수정합니다. 수정이 불가능한 경우 AMS는 인시던트를 생성합니다. 자동화로 문제가 해결되지 않는 경우 AMS는 인시던트 사례를 알리고 AMS 엔지니어가 참여합니다. 또한 이러한 알림은 이메일로 직접 전송할 수 있습니다(Direct-Customer-Alerts SNS 주제에 옵트인한 경우).

Application Load Balancer(ALB) 인스턴스	아니 요	RejectedConnectionCount 1분 동안 합계 > 0, 연속 5회.	CloudWatch는 로드 밸런서가 최대값에 도달하여 거부된 연결 수를 경보합니다.
Application Load Balancer(ALB) 대상	아니 요	TargetConnectionErrorCount 1분 동안 합계 > 0, 연속 5회.	로드 밸런서와 등록된 인스턴스 간에 연결 수가 설정되지 않은 경우 CloudWatch 경보가 발생합니다.
Amazon EC2 인스턴스 – Windows	아니 요	SecureChannelFailure 마지막 15개 데이터 포인트 중 10개에 대해 > 0.0.	채널 보안 연결이 실패할 때 경고하는 Windows 인스턴스의 CloudWatch 경보입니다.
Aurora 인스턴스	아니 요	CPUUtilization 5분 동안 > 85%, 연속 2회.	CloudWatch 경보.
AWS Backup	예	DeleteRecoveryPoint 예기치 않은 IAM 역할 보안 주체 또는 IAM 사용자 보안 주체가 AWS Backup 복구 시점을 삭제했습니다.	CloudWatch 이벤트. 백업 복구 시점이 삭제될 때 발생합니다.
AWS Outposts	예	AMSOupostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability	리소스의 인스턴스 패밀리 용량 가용성에 대한 CloudWatch 경보입니다 AWS Outposts .

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
EC2 인스턴스 - 모든 OSs	아니 요	= 5분 동안 80%, 연속 12회.	
		AMSOupostsInstanceTypeCapacityAvailability TypeCapacityAvailability	리소스의 인스턴스 유형 용량 가용성에 대한 CloudWatch 경보입니다 AWS Outposts .
		= 5분 동안 80%, 연속 12회.	
		AMSOupostsConnectedStatusC onnectedStatus	AWS Outposts 서비스 링크 연결에 대한 CloudWatch 경보가 1개 미만으로 손상되었습니다.
	아니 요	5분 동안 < 1, 연속 1회.	
		AMSOupostsCapacityExceptionCapacityExceptions	AWS Outposts리소스의 인스턴스 시작에 대한 용량 부족 오류에 대한 CloudWatch 경보 .
		5분 동안 0, 연속 1회.	
EC2 인스턴스 - 모든 OSs	아니 요	CPUUtilization*	CloudWatch 경보. CPU 사용률이 높다는 것은 데드락, 무한 루프, 악성 공격 및 기타 이상과 같은 애플리케이션 상태의 변화를 나타내는 지표입니다.
		5분 동안 >= 95%, 연속 6회.	
		StatusCheckFailed	CloudWatch 경보.
EC2 인스턴스 - 모든 OSs	아니 요	5분 동안 > 0, 연속 3회.	
		루트 볼륨 사용량	
EC2 인스턴스 - 모든 OSs	아니 요	5분 동안 >= 95%, 연속 6회.	

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
Amazon EC2 인스턴스 - Linux		루트가 아닌 볼륨 사용량 5분 동안 > 85%, 연속 2회. 기본적으로 비활성화되어 있습니다. 자세한 내용은 섹션을 참조하세요 https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info.	
		메모리 없음* MemoryFree 5분 동안 < 5%, 연속 6회.	
	예	EPS 맬웨어 인스턴스에서 맬웨어가 발견되었습니다.	CloudWatch 이벤트.
Amazon EC2 인스턴스 - Linux	아니 요	루트 볼륨 Inode 사용량 5분, 연속 6회 동안 평균 >= 95%.	CloudWatch 경보. Linux 인스턴스에만 적용됩니다.
		스왑 프리* 메모리 5분 동안 스왑 < 5%, 연속 6회.	

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
ElastiCache 클러스터	아니 요	CurrConnections = 65000	이 경보는 AMS에 ElastiCache 호스트의 최대 연결 제한을 알립니다. CloudWatch 경보. 이 임계값을 업데이트하려면 AMS 지원팀에 문의하십시오.

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
ElastiCache 노드	아니 요	CPUUtilization 평균 > 15분 동안 미리 정의된 값, 연 속 2회.	CloudWatch 경보. 기본값은 90입 니다. Redis인 경우 인스턴스 유 형에 따라 다음 값 중 하나를 사용 합니다. • cache.t1.micro: 90% • cache.m1.small: 90% • cache.m1.medium: 90% • cache.m1.large: 45% • cache.m1.xlarge: 22.5% • cache.m2.xlarge: 45% • cache.m2.4xlarge: 11.25% • cache.c1.xlarge: 11.25% • cache.t2.micro: 90% • cache.t2.small: 90% • cache.t2.medium: 45% • cache.m3.medium: 90% • cache.m3.large: 45% • cache.m3.xlarge: 22.5% • cache.m3.2xlarge: 11.25% • cache.r3.large: 45% • cache.r3.xlarge: 22.5% • cache.r3.2xlarge: 11.25% • cache.r3.4xlarge: 5.625% • cache.r3.8xlarge: 2.8125%
ElastiCac he 노드 - memcached	아니 요	SwapUsage 최대 > 50,000,000바이트, 5분, 5회 연속.	CloudWatch 경보. memcached에 만 적용됩니다.

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
OpenSearch 클러스터	아니 요	ClusterStatus.red 최대값은 1분, 연속 1회 동안 ≥ 1 입니다. AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	CloudWatch 경보. 하나 이상의 기본 샤드와 복제본이 노드에 할당되지 않았습니다. 자세한 내용은 빨간색 클러스터 상태를 참조하세요.
OpenSearch 도메인	아니 요	KMSKeyError ≥ 1 분, 연속 1회.	CloudWatch 경보. 도메인에서 저장된 데이터를 암호화하는 데 사용된 KMS 암호화 키가 비활성화되었습니다. 정상 작동으로 복원하려면 다시 활성화해야 합니다. 자세한 내용은 OpenSearch Service Service의 저장 데이터 암호화를 참조하세요.
		ClusterStatus.yellow 최대값은 1분, 연속 1회 동안 ≥ 1 입니다. AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	하나 이상의 복제 샤드가 노드에 할당되지 않았습니다. 자세한 내용은 노란색 클러스터 상태를 참조하세요.
		FreeStorageSpace 최소값은 1분, 연속 1회 동안 ≤ 20480 입니다. AMS는이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	클러스터 속 노드의 여유 스토리지 공간이 20GiB까지 떨어졌습니다. 자세한 내용은 사용 가능한 스토리지 공간 부족을 참조하세요.

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
		ClusterIndexWritesBlocked 5분 동안 ≥ 1, 연속 1회 AMS는 이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	클러스터가 쓰기 요청을 차단하고 있습니다. 자세한 내용은 ClusterBlockException을 참조하세요.
		노드 최소값은 1일 동안 $< x$, 연속 1회 AMS는 이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	x는 클러스터의 노드 수입니다. 이 경보는 클러스터에서 하나 이상의 노드가 하루 동안 연결되지 않았음을 나타냅니다. 자세한 내용은 실패한 클러스터 노드를 참조하세요.
		CPUUtilization 평균은 15분, 연속 3회 동안 $\geq 80\%$입니다. AMS는 이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	100% CPU 사용률이 일반적이지만 지속적으로 높은 평균은 문제가 됩니다. 더 큰 인스턴스 유형을 사용하거나 인스턴스 추가를 고려하세요.
		JVMMemoryPressure 최대값은 5분, 연속 횟수 3회 동안 $\geq 80\%$입니다. AMS는 이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	사용량이 늘어나면 클러스터에서 메모리 부족 오류가 발생할 수 있습니다. 수직 확장을 고려하세요. Amazon ES는 Java 힙에 인스턴스 RAM의 절반을 사용하고 힙 크기는 최대 32GiB입니다. 인스턴스를 최대 64GiB의 RAM까지 수직 확장할 수 있으며 인스턴스를 추가하면 수평 확장도 가능합니다.

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
		MasterCPUUtilization 평균은 15분, 연속 3회 동안 $\geq 50\%$ 입니다. AMS는 이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	전용 마스터 노드에 더 큰 인스턴스 유형을 사용하는 것이 좋습니다. 클러스터 안정성 및 블루/그린 배포에서의 역할 때문에 전용 마스터 노드는 데이터 노드보다 평균 CPU 사용량이 낮아야 합니다.
		MasterJVMMemoryPressure 최대값은 15분, 연속 1회 동안 $\geq 80\%$ 입니다. AMS는 이 알림이 트리거될 때 운영 영향을 줄이기 위해 사전 예방 조치를 취합니다.	전용 마스터 노드에 더 큰 인스턴스 유형을 사용하는 것이 좋습니다. 클러스터 안정성 및 블루/그린 배포에서의 역할로 인해 전용 마스터 노드는 데이터 노드보다 평균 CPU 사용량이 낮아야 합니다.
OpenSearch 인스턴스	아니 요	AutomatedSnapshotFailure 최대값은 1분, 연속 1회 동안 ≥ 1 입니다.	CloudWatch 경보. 자동 스냅샷에 오류가 발생했습니다. 이런 오류는 red 클러스터 상태로 인해 자주 발생했습니다. 빨간색 클러스터 상태를 참조하세요.
Elastic Load Balancing 인스턴스	아니 요	SurgeQueueLength 1분 동안 > 100, 연속 15회.	초과 요청 수가 라우팅 보류 중인 경우 CloudWatch 경보가 발생합니다.
		HTTPCode_ELB_5XX_Count 5분 동안 합계 > 0, 연속 3회.	로드 밸런서에서 시작된 초과 HTTP 5XX 응답 코드 수에 대한 CloudWatch 경보입니다.
		SpilloverCount 1분 동안 > 1, 연속 15회.	서지 대기열이 가득 차서 거부된 요청 수가 초과되면 CloudWatch 경보가 발생합니다.

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
GuardDuty 서비스	예	해당 사항 없음. 모든 조사 결과(위협 목적)가 모니터링됩니다. 각 결과는 알림에 해당합니다. GuardDuty 조사 결과의 변경 사항입니다. 이러한 변경은 새롭게 생성된 결과 또는 기존 결과의 후속 발생을 포함합니다.	지원되는 GuardDuty 결과 유형의 목록은 GuardDuty 활성 결과 유형에 있습니다 .
상태	다양	AWS Health Dashboard	AMS에서 지원하는 기존 서비스와 관련하여 AWS Health Dashboard (AWS Health) 이벤트의 상태가 변경되면 알림이 전송됩니다. 자세한 내용은 지원되는 서비스를 참조하세요 .
AWS Managed Microsoft AD	아니 요	Active Directory 상태 AWS Managed Microsoft AD 인스턴스가 활성 상태 이벤트를 보냅니다.	서비스 이벤트. 이벤트 후 디렉터리가 정상적으로 작동할 때 발생합니다.
		손상된 디렉터리 상태 AWS Managed Microsoft AD 인스턴스가 손상된 디렉터리 상태 이벤트를 보냅니다.	서비스 이벤트. 디렉터리가 성능 저하 상태에서 실행 중일 때 발생합니다. 1개 이상의 문제가 탐지되었고, 모든 디렉터리 작업이 전체 운영 용량에서 실행되지 못할 수 있습니다.
		사용할 수 없는 디렉터리 상태 AWS Managed Microsoft AD 인스턴스가 작동하지 않는 상태 이벤트를 보냅니다.	서비스 이벤트. 디렉터리가 작동하지 않을 때 발생합니다. 모든 디렉터리 엔드포인트가 문제를 보고했습니다.

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
		디렉터리 상태 삭제 AWS Managed Microsoft AD 인스턴스는 디렉터리 상태 이벤트 삭제를 전송합니다.	서비스 이벤트. 디렉터리가 현재 삭제 중일 때 발생합니다.
		실패한 디렉터리 상태 AWS Managed Microsoft AD 인스턴스가 실패 상태 이벤트를 보냅니다.	서비스 이벤트. 디렉터리를 생성할 수 없을 때 발생합니다.
		RestoreFailed Directory 상태 AWS Managed Microsoft AD 인스턴스는 복원 실패 디렉터리 상태 이벤트를 전송합니다.	서비스 이벤트. 스냅샷에서 디렉터리를 복원하지 못한 경우 내보내집니다.
Amazon RDS 인스턴스	아니 요	DB 인스턴스에 할당된 스토리지가 소진되면 스토리지 부족 알림이 트리거됩니다.	RDS-EVENT-0007, Amazon RDS 이벤트 알림 사용 의 세부 정보를 참조하세요.
		DB 인스턴스 실패 호환되지 않는 구성 또는 기본 스토리지 문제로 인해 DB 인스턴스에 장애가 발생했습니다. DB 인스턴스에 대해 특정 시점으로 복구를 시작합니다.	서비스 이벤트. RDS-EVENT-0031, Amazon RDS 이벤트 범주 및 이벤트 메시지 .
		장애 조치가 시도되지 않음 최근에 DB 인스턴스에 장애 조치가 발생하였기 때문에 Amazon RDS가 요청한 장애 조치를 실행하지 않습니다.	서비스 이벤트. RDS-EVENT-0034, Amazon RDS 이벤트 범주 및 이벤트 메시지 .

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
		DB 인스턴스 잘못된 파라미터 예를 들어 이 인스턴스 클래스의 메모리 관련 파라미터가 너무 높게 설정되어 MySQL이 시작하지 않습니다. 따라서 메모리 파라미터 설정을 변경한 후 DB 인스턴스를 재부팅하는 것이 바람직합니다.	서비스 이벤트. RDS-EVENT-0035, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		잘못된 서브넷 IDs 인스턴스 DB 인스턴스가 호환되지 않는 네트워크에 있습니다. 특정 서브넷 ID 중 일부가 잘못되었거나 존재하지 않습니다.	서비스 이벤트. RDS-EVENT-0036, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		DB 인스턴스 읽기 전용 복제본 오류 읽기 전용 복제 프로세스에서 오류가 발생하였습니다. 자세한 내용은 이벤트 메시지 단원을 참조하십시오. 읽기 전용 복제본 오류 문제 해결에 대한 자세한 내용은 MySQL 읽기 전용 복제본 문제 해결을 참조하세요.	서비스 이벤트. RDS-EVENT-0045, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		DB 인스턴스 읽기 복제 종료 읽기 전용 복제본에 대한 복제가 종료되었습니다.	서비스 이벤트. RDS-EVENT-0057, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		statspack 사용자 계정 생성 오류 Statspack 사용자 계정인 PERFSTAT 생성 중 오류가 발생하였습니다. Statspack 옵션을 추가하기 전에 계정을 삭제합니다.	서비스 이벤트. RDS-EVENT-0058, Amazon RDS 이벤트 범주 및 이벤트 메시지.

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
		DB 인스턴스 복구 시작 SQL Server DB 인스턴스가 미러를 재구성 중입니다. 이때 미러가 재구성 될 때까지 성능이 저하됩니다. 복구 모델이 FULL이 아닌 데이터베이스가 발견되었습니다. 복구 모델이 FULL로 다시 변경되었고 미러링 복구가 시작되었습니다(<dbname>: <recovery model found>[,...]).	서비스 이벤트. RDS-EVENT-0066, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		DB 클러스터에 대한 장애 조치가 실패했습니다.	RDS-EVENT-0069, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		잘못된 권한 복구 S3 버킷 SQL Server 기본 백업 및 복원을 위해 Amazon S3 버킷에 액세스하는 데 사용하는 IAM 역할이 잘못 구성되었습니다. 자세한 내용은 기본 백업 및 복원 설정을 참조하세요.	서비스 이벤트. RDS-EVENT-0081, Amazon RDS 이벤트 범주 및 이벤트 메시지.
		Aurora가 Amazon S3 버킷에서 백업 데이터를 복사할 수 없습니다.	RDS-EVENT-0082, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		DB 인스턴스가 할당된 스토리지의 90% 이상을 소비한 경우 스토리지 부족 알림	RDS-EVENT-0089, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		Aurora Serverless DB 클러스터에 대한 조정 실패 시 알림 서비스입니다.	RDS-EVENT-0143, Amazon RDS 이벤트 카테고리 및 이벤트 메시지의 세부 정보를 참조하세요.

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
		DB 인스턴스가 잘못된 상태입니다. 아무 조치도 필요하지 않습니다. 자동 확장은 나중에 다시 시도합니다.	RDS-EVENT-0219, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		DB 인스턴스가 스토리지 전체 임계값에 도달했으며 데이터베이스가 종료되었습니다.	RDS-EVENT-0221, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		이 이벤트는 RDS 인스턴스 스토리지 Autoscaling을 조정할 수 없으며 Autoscaling이 실패한 여러 이유가 있을 수 있음을 나타냅니다.	RDS-EVENT-0223, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		스토리지 자동 확장은 최대 스토리지 임계값에 도달하는 보류 중인 확장 스토리지 작업을 트리거했습니다.	RDS-EVENT-0224, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		DB 인스턴스에는 현재 가용 영역에서 사용할 수 없는 스토리지 유형이 있습니다. 자동 확장은 나중에 다시 시도합니다.	RDS-EVENT-0237, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		서브넷에서 사용할 수 있는 IP 주소가 충분하지 않기 때문에 RDS가 프록시 용량을 프로비저닝할 수 없습니다.	RDS-EVENT-0243, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		AWS 계정의 스토리지가 허용된 스토리지 할당량을 초과했습니다.	RDS-EVENT-0254, Amazon RDS 이벤트 범주 및 이벤트 메시지의 세부 정보를 참조하세요.
		CPUUtilization 15분 동안 평균 CPU 사용률 > 90%, 연속 2회.	CloudWatch 경보.

서비스:	보안 알림	알림 이름 및 트리거 조건	참고
		DiskQueueDepth 합계는 1분, 연속 15회 동안 > 75입니다. FreeStorageSpace 5분 동안 평균 < 1,073,741,824바이트, 연속 2회. SwapUsage 평균 >= 5분 동안 104,857,600바이트, 연속 2회.	
Amazon Redshift 클러스터	아니 요	RedshiftClusterStatus 유지 관리 모드가 아닌 경우 클러스터의 상태가 5분 동안 < 1입니다.	1은 정상 클러스터를 나타냅니다.
Amazon Macie	예	새로 생성된 알림 및 기존 알림에 대한 업데이트. Macie는 조사 결과에서 변경 사항을 찾습니다. 이러한 변경은 새롭게 생성된 결과 또는 기존 결과의 후속 발생을 포함합니다.	Amazon Macie 알림. 지원되는 Macie 알림 유형 목록은 Amazon Macie 조사 결과 분석을 참조하세요 . Macie는 모든 계정에 대해 활성화되어 있지 않습니다.

AMS는이 알림이 트리거될 때 사전 예방적 작업(클러스터 크기 조정)을 수행합니다.

문제 해결 노력에 대한 자세한 내용은 섹션을 참조하세요 [알림의 AMS 자동 문제 해결](#).

[Andrew의 동영상을 보고 자세히 알아보기\(7:03\)](#)

로그 보존 및 교체 기본값

이 섹션에서는 AMS 로그 관리 기본값을 설명합니다. 자세한 내용은 [로그 관리](#)를 참조하세요.

- 교체 = 인스턴스 내 로그 전환
- 보존 = Amazon CloudWatch Logs 및 Amazon Simple Storage Service(S3)에 로그를 보관하는 기간

로그는 필요에 따라 CloudWatch Logs(이를 구성할 수 있음) 및 S3에 보관됩니다. 만료되거나 삭제되지 않으며 서비스 내구성이 적용됩니다. 자세한 S3 내구성 정보는 [Amazon S3의 데이터 보호](#)를 참조하세요.

감사 및 보안상의 이유로 무기한 보관되는 로그를 제외한 모든 AWS CloudTrail 로그에 대한 로그 보존 변경을 요청할 수 있습니다.

로그 교체는 인스턴스 내에서 구성됩니다. 기본적으로 운영 체제 및 보안 로그는 100MB를 초과하는 경우 매시간 교체되며, 이는 인스턴스의 디스크에서 짧게 실행되지 않도록 하기 위해 수행됩니다.

인스턴스 내의 로그 에이전트는 로그를 CloudWatch Logs에 온라인으로 업로드하고, CloudWatch Logs에서 로그는 S3에 보관됩니다.

로그는 생성된 원시 형식으로 CloudWatch Logs 및 S3에 저장되며 사전 처리가 없습니다.

AMS 콘솔 사용

AWS 관리 콘솔의 AMS 콘솔을 사용하여 AMS와 상호 작용하고 AMS 고급 관리형 및 AMS Accelerate 리소스를 운영할 수 있습니다. AMS 콘솔은 일반적으로 모든 AWS 콘솔처럼 동작하지만 AMS는 프라이빗 조직이므로 AMS에 대해 활성화된 계정만 콘솔에 액세스할 수 있습니다. 계정에서 AMS가 활성화되면 통합 검색 창에서 "관리형 서비스"를 검색하여 콘솔에 액세스할 수 있습니다.

Note

계정 역할에 따라 AMS Advanced 콘솔 또는 AMS Accelerate 콘솔에 액세스합니다.

AMS 콘솔을 사용할 때는 다음 주의 사항에 유의하세요.

- AMS 콘솔은 계정별로 다릅니다. 따라서 조직의 "테스트" 계정에 있는 경우 해당 조직의 "Prod" 계정에서 리소스를 볼 수 없습니다. 마찬가지로 AMS Advanced 콘솔에 액세스하려면 AMS Advanced 역할이 있어야 합니다.
- AMS 콘솔은 인증 시 액세스할 수 있는 콘솔과 해당 콘솔에서 수행할 수 있는 작업을 결정하는 IAM 정책을 적용합니다. 관리자가 기본 AMS 정책에 추가 정책을 적용하여 콘솔에서 보고 수행할 수 있는 작업을 제한할 수 있습니다.

AMS Advanced 콘솔에는 다음과 같은 기능이 있습니다.

- 시작 페이지: 시작 페이지에는 기존 RFCs, 인시던트, 서비스 요청 및 보고서에 쉽게 액세스할 수 있는 정보 상자와 링크가 있습니다.
- 기능 페이지, 왼쪽 탐색 창의 링크:
 - 대시보드: 다음을 포함하여 계정의 현재 상태에 대한 개요를 제공합니다.
 - 변경 요청: 응답을 기다리는 RFCs 수를 확인하고 해당 필터가 활성화된 RFC 목록 페이지로 이동합니다. 승인을 기다리는 RFCs 수를 확인하고 해당 필터가 활성화된 RFC 목록 페이지로 이동합니다. 열려 있는 RFCs 확인하고 해당 필터가 활성화된 RFC 목록 페이지로 이동합니다. 모두 보기 링크를 클릭하여 RFCs 목록 페이지를 엽니다.
 - 인시던트: 응답을 기다리는 인시던트 사례 수를 확인하고 해당 필터가 활성화된 인시던트 목록 페이지로 이동합니다. 및 열린 수를 확인하고 해당 필터가 활성화된 인시던트 목록 페이지로 이동합니다. 모두 보기 링크를 클릭하여 인시던트 목록 페이지를 엽니다.
 - 서비스 요청: 응답을 기다리는 서비스 요청 수를 확인하고 해당 필터가 활성화된 서비스 요청 목록 페이지로 이동합니다. 및 열린 수를 참조하고 해당 필터가 활성화된 서비스 요청 목록 페이지로 이동합니다. 모두 보기 링크를 클릭하여 서비스 요청 목록 페이지를 엽니다.
 - 최근에 업데이트된 RFCs: 날짜, RFC 세부 정보에 대한 링크 및 상태
 - 최근에 생성된 인시던트 및 서비스 요청: 날짜, 사례 세부 정보에 대한 링크 및 유형(인시던트 또는 서비스 요청)
 - RFCs 계정의 기존 RFCs 목록을 엽니다.
 - 인시던트: 계정에 대해 열린 인시던트 목록을 엽니다.
 - 서비스 요청: 계정에 대해 열려 있는 서비스 요청 목록을 엽니다.
 - 보고서: 보고서 페이지와 기본 보고서, 일별 백업, 일별 패치 및 월별 청구를 엽니다.
 - 리소스:
 - VPCs 계정의 기존 VPCs 목록을 엽니다.
 - 스택: 계정의 기존 스택 목록을 엽니다.
 - AMIs 사용 가능한 AMS AMIs
 - 기능 스포트라이트: 콘솔의 최신 업데이트에 대한 정보
 - 개발자 리소스: AMS Advanced 변경 관리 SDK 등을 포함하여 다운로드 가능한 파일 페이지
 - 설명서: AWS Managed Services 설명서 랜딩 페이지

AMS API 및 CLI 사용

AWS Managed Services(AMS) API는 다른 AWS 서비스의 APIs. AMS API [참조에서 AMS API](#)에 대해 읽을 수 있습니다.

REST 호출을 위한 AMS API HTTP 엔드포인트

다양한 SDKs 외에도 AMS는 CLI를 제공합니다. AMS 엔드포인트에 대해 REST API 호출을 호출할 수도 있습니다.

두 개의 AMS APIs

- 변경 관리:이 API를 사용하여 RFCs 생성 및 업데이트, 새 인스턴스 배포, 인스턴스 업데이트 및 삭제, CTs에 대한 정보 가져오기, AMIs 생성 등 인프라에 대한 액세스 또는 변경을 요청합니다. HTTP 엔드포인트는 다음과 같습니다.

`https://amscm.us-east-1.amazonaws.com`

- SKMS:이 API를 사용하여 VPCs, 스택, 서브넷 및 AMIs를 포함한 인프라에 대한 정보를 가져옵니다. HTTP 엔드포인트는 다음과 같습니다.

`https://amsskms.us-east-1.amazonaws.com`

AMS CLI 설치 또는 업그레이드

AMS CLI는 AMS API와 쉽게 상호 작용할 수 있는 방법이며 이 섹션의 예제에서 사용됩니다. AWS CLI 및 AMS CLI에 대한 사용 규칙은 [AWS 명령줄 인터페이스 사용을 참조하세요](#).

SAML 설치에 대한 자세한 내용은 섹션을 참조하세요 [AD FS 클레임 규칙 및 SAML 설정](#).

AMS CLI를 설치하거나 업그레이드하려면 다음 지침을 따르세요.

Note

이 절차를 수행하려면 관리자 자격 증명이 있어야 합니다.

AWS CLI는 AWS Managed Services(AMS) CLIs(변경 관리 및 SKMS)를 사용하기 위한 사전 조건입니다.

1. AWS CLI를 설치하려면 [AWS 명령줄 인터페이스 설치](#)를 참조하고 적절한 지침을 따릅니다. 해당 페이지 하단에는 [Linux](#), [MS Windows](#), [macOS](#), [가상 환경](#), [번들 설치 관리자\(Linux, macOS 또는 Unix\)](#) 등 다양한 설치 프로그램을 사용하기 위한 지침이 있습니다.

설치 후를 실행 `aws help`하여 설치를 확인합니다.

2. AWS CLI가 설치되면 AMS CLI를 설치하거나 업그레이드하려면 AMS CLI 또는 AMS SDK 배포 가능 zip 파일을 다운로드하고 압축을 풉니다. AMS 콘솔 왼쪽 탐색 창의 [개발자 리소스](#) 링크를 통해 AMS CLI 배포 파일에 액세스할 수 있습니다.
3. README 파일은 모든 설치에 대한 지침을 제공합니다.

다음 중 하나를 엽니다.

- CLI zip: AMS CLI만 제공합니다.
- SDK zip: 모든 AMS APIs와 AMS CLI를 제공합니다.

Windows의 경우 적절한 설치 관리자(32비트 또는 64비트 시스템만 해당)를 실행합니다.

- 32비트: ManagedCloudAPI_x86.msi
- 64비트: ManagedCloudAPI_x64.msi

Mac/Linux의 경우 명령을 실행하여 `AWSManagedServices_InstallCLI.sh`라는 파일을 실행합니다. `sh AWSManagedServices_InstallCLI.sh`. `amscm` 및 `amsskms` 디렉터리와 해당 콘텐츠는 `AWSManagedServices_InstallCLI.sh` 파일과 동일한 디렉터리에 있어야 합니다.

4. 기업 자격 증명을 AWS와의 페더레이션(AMS 기본 구성)을 통해 사용하는 경우 페더레이션 서비스에 액세스할 수 있는 자격 증명 관리 도구를 설치해야 합니다. 예를 들어 AWS 보안 블로그 [SAML 2.0 및 AD FS를 사용하여 연합 API 및 CLI 액세스를 구현하는 방법](#)을 사용하여 자격 증명 관리 도구를 구성할 수 있습니다.
5. 설치 후 `aws amscm help` 및 `aws amsskms help`하여 명령과 옵션을 확인합니다.

Note

이러한 명령이 작동하려면 AMS CLI가 설치되어 있어야 합니다. AMS API 또는 CLI를 설치하려면 AMS 콘솔 개발자 리소스 페이지로 이동합니다. AMS CM API 또는 AMS SKMS API에 대한 참조 자료는 사용 설명서의 AMS 정보 리소스 섹션을 참조하세요. 인증 `--profile` 옵션을 추가해야 할 수 있습니다. 예: `aws amsskms ams-cli-command --`

profile SAML. 와 같이 모든 AMS 명령이 us-east-1에서 실행되므로 --region 옵션을 추가해야 할 수도 있습니다.

```
aws amscm ams-cli-command --region=us-east-1.
```

CLI, Ruby, Python 및 Java에서 AMS API 사용

다음은 사용 가능한 모든 언어로 된 AMS API ListChangeTypeClassificationSummaries 작업에 대한 코드 조각 목록입니다.

Python, Ruby 및 Java SDKs의 경우 [Amazon Web Services용 도구](#)를 참조하고 SDKs 섹션까지 아래로 스크롤합니다. 각 SDK 설치 관리자에는 추가 코드 조각이 있는 README가 포함되어 있습니다.

AMS API에서 CLI로 예제

AMS CLI를 설치한 후(AWS CLI 필요, 참조 [AMS CLI 설치 또는 업그레이드](#)) 먼저 호출을 재구성하여 AMS API 또는 aws amscm를 지정한 다음 aws amsskms낙타 대소문자를 대체하는 하이픈으로 작업을 제공하여 모든 AMS API 작업을 실행할 수 있습니다. 마지막으로 SAML과 같은 자격 증명을 제공합니다.

자세한 내용은 [AWS 명령줄 인터페이스 사용을 참조하세요](#).

예시

- API: 'ChangeTypeClassificationSummaries[
[Category,Subcategory,Item,Operation,ChangeTypeId]'
- CLI: amscm list-change-type-classification-summaries
--query "ChangeTypeClassificationSummaries[*].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table

Note

SAML로 인증하는 경우 명령의 시작 aws --profile saml 부분에 추가합니다. 예:

```
aws --profile saml amscm list-change-type-classification-  
summaries --query "ChangeTypeClassificationSummaries[*].  
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

AMS API에서 Python으로의 예제

Python과 함께 AMS API를 사용하려면 AMS CLI를 설치하고 boto3를 설치합니다. 다음 단계를 따릅니다.

1. AMS CLI를 설치합니다. [AMS CLI 설치 또는 업그레이드](#)을(를) 참조하세요.
2. AWS SDK for Python인 boto3를 설치합니다. 자세한 내용은 이 블로그 게시물 [Now Available – AWS SDK for Python \(Boto3\)](#)을 참조하세요.

```
import boto3
```

3. AMS Change Management 클라이언트를 가져옵니다.

```
cm = boto3.client('amscm')
```

4. AMS CTs 가져오기:

```
cts = cm.list_change_type_classification_summaries()

print(cts)
```

Python 예제

다음은 AMS에서 Python을 사용하여 EC2 인스턴스를 생성하거나 Lambda를 사용하는 몇 가지 예입니다.

EC2를 생성하는 Python 예제

이 예제에서는 Python 코드 내에서 amscm RESTful API를 사용하여 파일을 제출하고 RFC 프로세스를 수행하는 방법을 보여줍니다.

1. 액세스 권한이 있는 위치에 AMS CLI를 설치합니다. AMS CLI가 제공하는 파일이 필요합니다.
2. Python 라이브러리를 호출하고 EC2 인스턴스를 생성합니다.

```
import boto3
import json
import time

# Create the amscm client
cm = boto3.client('amscm')
```

```
# Define the execution parameters for EC2 Create
AMSExecParams = {
    "Description": "EC2-Create",
    "VpcId": "VPC_ID",
    "Name": "My-EC2",
    "TimeoutInMinutes": 60,
    "Parameters": {
        "InstanceAmiId": "INSTANCE_ID",
        "InstanceSubnetId": "SUBNET_ID"
    }
}

# Create the AMS RFC
cts = cm.create_rfc(
    ChangeTypeId="ct-14027q0sjyt1h",
    ChangeTypeVersion="3.0",
    Title="Python Code RFC Create",
    ExecutionParameters=json.dumps(AMSExecParams)
)

# Extract the RFC ID from the response
NewRfcID = cts['RfcId']

# Submit the RFC
RFC_Submit_Return=cm.submit_rfc(RfcId=NewRfcID)

# Check the RFC status every 30 seconds
RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']

while RFC_Status_Code != "Success":
    if RFC_Status_Code == "PendingApproval":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "InProgress":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "Failure":
        print(RFC_Status_Code)
        break
    else:
        print(RFC_Status_Code)

    RFC_Status = cm.get_rfc(RfcId=NewRfcID)
```



```
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']
```

Lambda를 사용한 Python 예제

이 예제에서는 AMS 모델을 코드와 번들링하여 Lambda 또는 EC2와 함께 사용할 수 있도록 하는 방법을 보여줍니다. 를 설치할 수 없거나 설치할 수 없는 위치입니다 `amsccli`.

Note

AMS는 가져올 수 있는 AMS별 Python SDK를 제공하지 않습니다. `amsccli` 설치 스크립트는 CLI의 일반 경로에 AMS 서비스 데이터 모델을 설치합니다. CLI 사용 및 시스템 Python 사용의 경우 `awscli` 및 모두 동일한 기본 위치()에서 서비스 모델을 `boto3` 읽기 때문에 괜찮습니다. `~/.aws/models`. 그러나 Lambda의 `boto3`(또는 로컬이 아닌 다른 런타임)를 통해 AMS 서비스를 사용하려는 경우 데이터 모델이 더 이상 없기 때문에 중단됩니다. 다음은 데이터 모델을 함수로 패키징하여이 문제를 해결하는 방법입니다.

Lambda 또는 EC2, Fargate 등과 같은 다른 런타임에서 AMS 통합 Python 코드를 실행하기 위해 수행할 수 있는 간단한 단계가 있습니다. 다음 워크플로는 AMS 통합 Lambda 함수에 필요한 단계를 보여줍니다.

코드의 배포 패키지에 데이터 모델을 추가하고 SDK 검색 경로를 업데이트하면 SDK 환경을 시뮬레이션할 수 있습니다.

Important

이 예제와 표시된 모든 비 Python 명령은 Mac 컴퓨터에서 테스트되었습니다.

워크플로 예제:

1. `amsccli`를 설치합니다. 이렇게 하면 컴퓨터(Mac)의 `~/.aws/models`에 폴더가 생성됩니다.
2. 모델을 로컬 디렉터리에 복사합니다 `cp ~/.aws/models ./models`.
3. 모델을 코드의 배포 패키지에 포함합니다.
4. 함수 코드를 업데이트하여 SDK 경로에 새 모델을 추가합니다. `boto3` 또는 `botocore`를 가져오려면 먼저이 코드를 실행해야 합니다.

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note

예제 모델은 라는 디렉터리에 있으므로 `AWS_DATA_PATH=./models`에 `models`를 추가합니다. 디렉터리 이름이 인 경우 다음 코드를 추가합니다 `/ams/boto3models`.

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

코드가 AMS 모델을 성공적으로 찾아야 합니다. 패키징에 대한 보다 구체적인 예로 Lambda별 워크플로가 있습니다.

AMS Lambda 워크플로 예제:

이 단계는 위의 일반 예제를 AWS Lambda 함수 생성에 적용합니다.

1. `amscli`를 설치합니다. 이렇게 하면 컴퓨터(Mac)의 `~/.aws/models`에 폴더가 생성됩니다.
2. 모델을 로컬 디렉터리에 복사합니다.

```
cp ~/.aws/models ./models
```

3. 함수의 배포 zip 파일에 모델을 추가합니다.

```
zip -r9 function.zip ./models
```

Important

함수 코드를 업데이트하여 SDK 경로에 새 모델을 추가합니다. `boto3` 또는 `botocore`를 가져오려면 먼저 이 코드를 실행해야 합니다.

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note

예제 모델은 라는 디렉터리에 있으므로 AWS_DATA_PATH./models에를 models추가합니다. 디렉터리 이름이 인 경우 다음 코드를 추가합니다/ams/boto3models.

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

이제 함수를 배포합니다.

1. 배포 zip 파일에 함수 코드를 추가합니다(아직 추가하지 않은 경우).

```
zip -g function.zip lambda-amscm-test.py
```

2. 생성한 zip 파일(콘솔 또는 CLI)을 사용하여 함수를 생성하거나 업데이트합니다.

```
aws lambda update-function-code --function-name lambda-amscm-test --zip-file fileb://
function.zip --region us-east-1
```

이제 AMS 통합 Python Lambda가 작동합니다.

Note

함수에 대한 IAM 권한이 amscm 있거나 권한 오류가 발생해야 합니다.

amscm(lambda-amscm-test.py 콘텐츠)을 테스트하기 위한 샘플 Lambda 함수 코드:

```
import json

# Force lambda to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore

def lambda_handler(event, context):
    use_session = boto3.session.Session(region_name="us-east-1")
    try:
        cm = use_session.client("amscm")
        cts = cm.list_change_type_categories()
        print(cts)
    except botocore.exceptions.UnknownServiceError:
        print("amscm not found")

    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

테스트 출력(성공):

함수 응답:

```
{
  "statusCode": 200,
  "body": "\"Hello from Lambda!\""
}
```

Request ID:
"1cea13c0-ed46-43b1-b102-a8ea28529c27"

함수 로그:

```
START RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27 Version: $LATEST
{'ChangeTypeCategories': ['Deployment', 'Internal Infrastructure Management',
  'Management'], 'ResponseMetadata': {'RequestId': 'e27276a0-e081-408d-
bcc2-10cf0aa19ece', 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid':
```

```
'e27276a0-e081-408d-bcc2-10cf0aa19ece', 'content-type': 'application/x-amz-json-1.1',  
'content-length': '89', 'date': 'Sun, 10 May 2020 23:21:19 GMT'}, 'RetryAttempts': 0}}  
END RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27
```

AMS API에서 Ruby로 예제

Ruby와 함께 AMS API를 사용하려면 AWS Ruby SDK 및 AMS CLI를 설치합니다. 다음 단계를 따릅니다.

1. AMS CLI를 설치합니다. [AMS CLI 설치 또는 업그레이드](#)을(를) 참조하세요.
2. AWS Ruby SDK를 설치합니다. [Amazon Web Services용 도구를](#) 참조하세요.
3. 다음 명령을 사용하여 Ruby를 구성합니다.

```
require 'aws-sdk'  
  
config = {  
  region: 'us-east-1',  
  credentials: Aws::Credentials.new('ACCESS_KEY', 'SECRET_KEY')}
```

4. AMS CTs 가져오기:

```
ams_cm = Aws::amscm::Client.new(config)  
  
cts = ams_cm.list_change_type_classification_summaries  
  
print(cts)
```

AMS API에서 Java로 예제

AMS API를 Java와 함께 사용하려면 AWS Java SDK 및 AMS CLI를 설치합니다. 다음 단계를 따릅니다.

1. AMS CLI를 설치합니다. [AMS CLI 설치 또는 업그레이드](#)을(를) 참조하세요.
2. AWS Java SDK를 설치합니다. [Amazon Web Services용 도구를](#) 참조하세요.
3. 다음 명령을 사용하여 Java를 구성합니다.

```
import com.amazonaws.auth.BasicAWSCredentials;  
  
import com.amazonaws.services.amscm.model.AWSManagedServicesCMClient;
```

```
import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesReque

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesResult
```

```
public static void getChangeTypeClassificationSummaries() {
```

4. 자격 증명을 설정합니다. 이를 하드코딩하지 않는 것이 좋습니다.

```
final BasicAWSCredentials awsCredsCm =

    new BasicAWSCredentials("ACCESS_KEY", "SECRET_KEY");
```

5. AMS Change Management 클라이언트를 생성합니다.

```
final AWSManagedServicesCMClient cmClient =

    new AWSManagedServicesCMClient(awsCredsCm);
```

6. AMS CTs 가져오기:

```
final ListChangeTypeClassificationSummariesRequest listCtsRequest = new
ListChangeTypeClassification SummariesRequest();

final ListChangeTypeClassificationSummariesResult listCtsResult =

cmClient.listChangeTypeClassificationSummaries(listCtsRequest);

System.out.println("List of CTs");

listCtsResult.getChangeTypeClassificationSummaries().stream()

.map(x -> x.getCategory() + "/" + x.getSubcategory() + "/" +
x.getItem() + "/" + x.getOperation())

.forEach(System.out::println);

}
```

AMS에서 자체 EPS 사용

AMS "자체 엔드포인트 보안 제공"(BYOEPS) 기능을 사용하여 기본 Trend Micro Deep Security 에 이전트를 자체 엔드포인트 보안 솔루션 또는 Trend Micro 라이선스로 바꿉니다. Trend Micro Deep Security 이외의 제품에 대한 비용 효율적인 라이선스가 이미 있거나 EPS를 제공하는 팀이 있거나 특정 EPS 도구를 사용하려는 경우 인스턴스에서 BYOEPS를 사용합니다.

BYOEPS는 계정 수준에서 작동합니다. 계정의 인스턴스는 BYOEPS 또는 기본 AMS 관리형 EPS를 사용합니다.

- 다중 계정 랜딩 존(MALZ): BYOEPS 또는 관리형 EPS를 사용하는 애플리케이션 계정을 지정합니다.
- 단일 계정 랜딩 존(SALZ): AMS 계정은 BYOEPS 또는 관리형 EPS를 사용합니다.

BYOEPS는 Trend Micro Deep Security AWS 비용을 절감합니다. 액세스 관리(배스천 및 관리 호스트)에 필요한 AMS 생성 및 유지 관리 EC2 인스턴스를 보호하려면 AMS 관리형 EPS가 여전히 필요하기 때문에 EPS 비용은 계속 발생합니다. 총 비용 영향을 계산하려면 새 도구의 라이선스 비용과 필요한 서비스 수준에서 EPS를 관리하는 비용을 고려해야 합니다.

BYOEPS를 사용하면 보안 관리에 대한 AMS 역할과 책임이 변경됩니다.

- R은 작업을 수행하기 위해 작업을 수행하는 책임 당사자를 나타냅니다.
- C는 컨설팅, 일반적으로 주제 전문가로서 의견을 구하는 당사자, 양자 간 커뮤니케이션이 있는 당사자를 의미합니다.
- 나는 정보, 즉 종종 작업 또는 결과물 완료 시에만 진행 상황에 대한 정보를 받는 당사자를 의미합니다.

보안 관리	Customer	AWS Managed Services
AMS 공유 서비스의 EC2 인스턴스용 Managed EPS의 유효한 라이선스 유지	R	C
AMS 공유 서비스의 EC2 인스턴스에 대한 관리형 EPS 구성	정보	R

보안 관리	Customer	AWS Managed Services
AMS 공유 서비스의 EC2 인스턴스에 대한 관리형 EPS 업데이트	정보	R
AMS 공유 서비스의 EC2 인스턴스에서 맬웨어 모니터링	정보	R
AMS 공유 서비스의 EC2 인스턴스에 대한 바이러스 서명 유지 관리 및 업데이트	정보	R
AMS 공유 서비스의 EC2 인스턴스에 대한 맬웨어로 감염된 인스턴스 문제 해결	C	R

BYOEPS를 사용하면 AMS에서 제공하는 보안 제어 중 하나가 손실됩니다. Amazon GuardDuty, Amazon Macie와 같은 도구와 IAM 구성 검토와 같은 프로세스 제어를 통해 보안 관리가 계속 제공됩니다. BYOEPS 사용은 AMS 규정 준수 인증 및 증명에 영향을 주지 않습니다. 그러나 많은 보안 프레임워크 및 인증에는 맬웨어 및 악성 코드로부터 보호하기 위한 요구 사항이 있습니다. 계정을 안전하게 유지하고 규정을 준수할 수 있도록 계획된 제어를 평가하여 워크로드의 규정 준수 인증에 대한 보안 요구 사항을 충족하는지 확인합니다.

계정에 대해 BYOEPS 활성화

BYOEPS를 켜는 프로세스는 세 단계로 구성되며 여러 RFCs 사용합니다. BYOEPS를 켜는 데 필요한 세 단계에 대해 알아보려면 다음 정보를 검토하세요. 그런 다음 CSDM과 조정하여 계정에 대해 BYOEPS를 켭니다.

주제

- [1단계: 사전 조건](#)
- [2단계: 계정에서 BYOEPS 활성화](#)
- [3단계: 인스턴스 마이그레이션](#)

1단계: 사전 조건

- 기본 Amazon EC2 인스턴스 프로파일은 `customer-mc-ec2-instance-profile`입니다. 기본 프로파일 외에도 다른 Amazon EC2 인스턴스 프로파일을 사용하는 경우 `/ams/end-point-security` 리소스에 대한 `ssm:GetParameter` 작업을 EC2 인스턴스 프로파일로 허용합니다.

EC2 인스턴스 프로파일을 업데이트할 수 없는 경우 업데이트해야 하는 인스턴스 프로파일을 지정하는 RFC를 제출합니다.

- 이 변경의 범위를 이해합니다.

AMS 자동 변경 유형(CT)을 통한 배포를 통해 생성에 사용되는 AMI를 지정할 수 있습니다.

AMS 관리형 EPS를 사용하는 계정에서 BYOEPS를 사용하려면 AMS와 협력하여 해당 EC2 인스턴스에서 Trend Micro 에이전트를 제거하고 해당 인스턴스에서 AMS 코드(예: 부팅 스크립트)를 업데이트해야 합니다. 이러한 작업을 수행하려면 재부팅이 필요할 수 있으므로 유지 관리 기간의 일부로 이러한 작업을 수행하는 것이 가장 좋습니다. CSDM에 문의하여 이 활동을 수행하고 마이그레이션 계획을 생성할 유지 관리 기간을 식별합니다. 마이그레이션 계획의 경우 다음 질문을 고려하세요.

- 마이그레이션해야 하는 인스턴스 수는 몇 개입니까? 총 인스턴스 수를 더 작은 증분 배치로 나눕니다.
 - 인스턴스를 배치로 나누려면 어떻게 해야 합니까? 예를 들어 리소스 그룹으로 나누고 목록을 생성하여 AMS 운영 팀과 공유할 수 있습니다.
 - 각 배치에는 시간이 얼마나 걸리나요? 총 시간이 얼마나 필요합니까? 동일한 유지 관리 기간에 원하는 EPS 도구를 설치할 수 있습니다. 시간이 얼마나 걸리나요?
- CSDM은 마이그레이션 계획을 AMS 운영 팀과 공유합니다. 인스턴스 풀릿이 50을 초과하는 경우 CSDM과 협력하여 계획된 이벤트 관리(PEM) 프로세스를 사용하여 계획된 이벤트를 생성합니다. 자세한 내용은 [AWS Managed Services의 계획된 이벤트 관리](#) 섹션을 참조하세요.

AMS Operations는 CSDM과 조정하고 계정의 인스턴스 수에 따라 유지 관리 기간에 따라 RFCs를 제출하는 방법을 조언합니다.

- 2020년 12월 이후에 릴리스된 AMS AMI를 사용하도록 사용자 지정 또는 AMS AMI를 사용하여 EC2 인스턴스 시작 자동화 또는 프로세스를 업데이트합니다. AMIs AMIs

2단계: 계정에서 BYOEPS 활성화

계정에서 BYOEPS를 사용하면 보안 관리에 대한 AMS의 책임이 변경됩니다. BYOEPS를 활성화하기 전에 보안 및 클라우드 플랫폼 팀에 문의하십시오.

계정에 BYOEPS를 요청하려면 다음 세부 정보와 함께 ct-0xdawir96cy7k를 사용하여 "MOO" 업데이트 RFC(관리 | 기타 | 기타 | 업데이트)를 제출합니다.

Please enable BYOEPS for this account/these accounts
Account IDs: *IDs for the accounts for BYOEPS.*

AMS는 파라미터 스토어 업데이트를 계정에 배포하고 [Amazon EC2 IAM 인스턴스 프로파일을](#) 업데이트합니다.

Note

- 최신 AMS AMIs를 사용하는 새 인스턴스가 시작된 계정은 Trend Micro 에이전트 설치를 건너뛸 수 있습니다. 2020년 12월 이전 AMIs BYOEPS 기능을 지원하지 않습니다. 이전 AMIs 사용하는 자동화를 업데이트하여 BYOEPS 기능 지원과 함께 최신 AMS AMIs 사용합니다.
- 기존 EC2 인스턴스 처리는 3단계: 인스턴스 마이그레이션을 참조하세요.

3단계: 인스턴스 마이그레이션

사용 사례에 따라 다음 옵션 중 하나를 사용하여 인스턴스를 마이그레이션합니다. 어떤 옵션을 선택해야 할지 잘 모르는 경우 CA 또는 CSDM에 문의하십시오.

AMS 관리형 EPS를 사용하는 EC2 인스턴스가 있는 계정

유지 관리 기간 동안 1단계의 계획에 따라 BYOEPS에 온보딩해야 하는 각 인스턴스에 대해 다음 작업이 수행됩니다.

- AMS에서 수행: AMS 코드(부트 스크립트, 모듈 등)를 최신 버전으로 업데이트합니다. 이는 이전 AMS 부팅 스크립트에 BYOEPS 기능 지원이 없고 부팅할 때마다 Trend Micro 에이전트를 다시 설치하기 때문에 필요합니다. 또한 Trend Micro Agent를 제거합니다.
- 사용자가 수행: 선호하는 EPS 도구를 설치하고 구성합니다.

Important

Trend Micro Agent는 맬웨어 보호를 제공합니다. 인스턴스를 보호하기 위해 적절한 교체를 설치해야 합니다.

이러한 변경을 수행하려면 변경 유형 ct-2iz9nvw8zlhst인 RFCs를 배치<https://docs.aws.amazon.com/managedservices/latest/ctref/management-host-trend-micro-dsm-remove-trend-micro-eps-agent-review-required>로 제출합니다.

AMS 관리형 EPS를 사용하는 EC2 인스턴스가 없는 계정

최신 AMS AMIs를 사용하는 새 인스턴스가 시작된 계정은 Trend Micro 에이전트 설치를 건너뛸 수 있습니다. 2020년 12월 이전 AMIs BYOEPS 기능을 지원하지 않습니다. 이전 AMIs 사용하는 자동화를 업데이트하여 BYOEPS 기능 지원과 함께 최신 AMS AMIs 사용합니다.

EC2 인스턴스에 에이전트 추가

AMS 패턴을 사용하여 CrowdStrike 또는 Qualys, 서비스 요청 제출과 같은 도구의 에이전트를 배포할 수 있습니다.

AMS 알림 수신

사용자와 AMS 간의 통신은 다음과 같은 여러 가지 이유로 발생합니다.

- 승인이 필요한 AMS에서 생성한 RFC
- 생성한 RFC를 조사하기 위해 생성한 AMS 사례로 실패한 경우
- 모니터링 알림으로 생성된 이벤트
- 예정된 패치를 알려주는 패치 서비스 알림
- 서비스 요청 및 인시던트 보고서
- 월별 CRM 보고서
- 가끔 중요한 AWS 공지 사항(사용자 측에 조치가 필요한 경우 CSDM에서 연락)

이러한 모든 알림은 온보딩 시 AMS에 제공한 기본 연락처 정보(루트 계정 이메일)로 전송됩니다. 개별 이메일을 최신 상태로 유지하기 어렵기 때문에 나중에 업데이트할 수 있는 그룹 이메일을 사용하는 것이 좋습니다. 사용자에게 전송된 모든 알림은 AMS 작업에서도 수신되며 응답을 하기 전에 분석됩니다.

AMS 알림 서비스는 알림을 위한 연락처를 설정하는 두 가지 추가 방법을 제공합니다.

- 리소스에 연락처 태그(연락처 정보인 키 값 태그)를 지정하고 CSDM에 키 이름 태그를 제공합니다. 이러한 리소스에 대한 경보는 온보딩 시 생성된 계정 연락처 외에도 키 값에 제공된 연락처로 전송됩니다. 이는 애플리케이션 소유자에게 특히 유용합니다. 자세한 내용은 [태그 기반 알림](#) 단원을 참조하십시오.

- (온보딩 시 필수) 리소스 기반이 아닌 알림에 대한 연락처 목록을 CSDM에 전송합니다. 예를 들어 "SecurityContacts"라는 목록과 "OperationsContacts"라는 다른 목록이 있을 수 있습니다. AMS는 알림 서비스에 목록을 추가하고 해당 목록의 컨텍스트에 적용되는 경보가 해당 연락처로 전송됩니다. 이는 조직 문제에 특히 유용합니다.

이 고급 알림 라우팅 기능은 Amazon EC2 인스턴스 장애, Amazon Elastic Block Store(Amazon EBS) 볼륨 용량 사용률 - 루트 사용량, Amazon EBS NonRoot 사용량, 높은 메모리 사용률, 높은 스왑 사용량, Amazon EC2의 높은 CPU 사용률과 같은 대부분의 필수 CloudWatch 경보에 대해 활성화됩니다.

또한 서비스 요청 또는 인시던트 보고서를 제출할 때 "CC Emails"(권장)를 추가할 수 있으며 해당 이메일 주소는 서비스 요청 또는 인시던트에 대한 알림을 수신합니다.

Important

서비스 요청 및 인시던트 보고서에 제공된 CC 이메일 주소는 통신에 대한 이메일 알림을 수신하지만, 알림을 패치하는 등의 다른 알림은 알림을 기다리고 있다는 명시적 알림 없이 서비스 요청 목록에 표시됩니다(이메일도 기본 연락처로 전송됨). 따라서 가능한 경우 CC 이메일을 추가하고 AMS를 사용하는 모든 사용자가 멤버인 그룹으로 기본 연락처 이메일을 설정하는 것이 좋습니다.

또한 새 AMIs, RFC 상태 변경 및 AMS 계정의 구성 변경에 대한 특별 알림을 요청할 수 있습니다. 이러한 선택적 알림 서비스는 다음에 설명합니다.

SNS를 사용한 AMS AMI 알림

AMS는 AMI 알림 서비스를 제공합니다. 이를 사용하여 AMS AMI 업데이트가 릴리스되었을 때 알려주는 Amazon Simple Notification Service(SNS) 주제를 구독할 수 있습니다. 사용하는 AMS AMIs에 대한 알림만 수신하도록 선택하거나 모든 AMS AMIs. SNS 주제에 대한 자세한 내용은 [Amazon Simple Notification Service란 무엇입니까?](#)를 참조하세요.

AMIs 릴리스될 때마다 해당 주제의 구독자에게 알림을 보냅니다.이 섹션에서는 AMS AMI 알림을 구독하는 방법을 설명합니다.

샘플 메시지

```
{
  "Type" : "Notification",
  "MessageId" : "example messageId",
```

```

"TopicArn" : "arn:aws:sns:us-east-1:591688410472:customer-ams-windows2019",
"Subject" : "New AMS AMIs are Now Available",
"Message" : "{\"v1\": {\"Message\": \"A new version of the AMS Amazon Machine Images has
been released. You are now able to launch new EC2 stacks from these AMIs.
Please use this time to update any dependencies such as CloudFormation or Autoscaling
groups. Release Notes Windows - Contains latest Windows Patches:
Microsoft Windows Server 2008 R2 Datacenter - (KB2819745, KB3018238, KB4507004,
KB4507437) Microsoft Windows Server 2016 Datacenter Security Enhancedn - (KB4509091,
KB4507459)
Microsoft Windows Server 2016 Datacenter - (KB4509091, KB4507459) Microsoft Windows
Server 2012 R2 Security Enhancedn - (KB3191564, KB3003057, KB3013172, KB3185319,
KB4504418,
KB4506996, KB4507463) Microsoft Windows Server 2012 R2 Standardn - (KB3003057,
KB3013172, KB3185319, KB4504418, KB4506996, KB4507463) Linux - Contains latest Linux
patches -
All AMIs now force domainjoin-cli leave before domainjoin-cli join for better
stability in the domain join process.\"\", \"images\":
{\"images\": {\"image_name\": \"customer-ams-windows2019-2021.08-1\", \"image_id\":
\"ami-05dfa45396fddaa5e\"}}, \"region\": \"us-east-1\"}}\",
\"Timestamp\" : \"2021-09-03T19:05:57.882Z\",
\"SignatureVersion\" : \"1\",
\"Signature\" : \"example sig\",
\"SigningCertURL\" : \"example url\",
\"UnsubscribeURL\" : \"example url\"
}

```

다음은 구독할 수 있는 AMS AMI 주제:

- ALL:를 사용합니다customer-ams-all-amis. 이 주제 구독은 AMS AMIs가 업데이트되면 알려줍니다.
- AMS AWS Linux AMIs: Amazon Linux의 경우 customer-ams-amazon1 및를 사용합니다customer-ams-amazon1-security-enhanced. Amazon Linux 2의 경우 customer-ams-amazon2 및를 사용합니다customer-ams-amazon2-security-enhanced.
- AMS SUSE Linux AMIs: customer-ams-sles12 또는를 사용합니다customer-ams-sles15.
- AMS AWS RedHat AMIs customer-ams-rhel8, customer-ams-rhel8-security-enhanced, customer-ams-rhel7,를 사용합니다customer-ams-rhel7-security-enhanced.
- AMS AWS CentOS AMIs: customer-ams-centos7,를 사용합니다customer-ams-centos7-security-enhanced.
- AMS Ubuntu AMIs:를 사용합니다customer-ams-ubuntu18.

- AMS AWS Windows AMIs: customer-ams-windows2019, , customer-ams-windows2019-security-enhanced, customer-ams-windows2016, customer-ams-windows2016-security-enhanced, customer-ams-windows2012, customer-ams-windows2012r2-security-enhanced, customer-ams-windows2012r2를 사용합니다customer-ams-windows2022.

Amazon SNS 콘솔을 사용하여 AMS 새 AMI 알림을 구독하려면:

1. Amazon SNS 콘솔의 [대시보드](#)를 엽니다.
2. 오른쪽 상단 모서리에서 구독하려는 AMIs의 AWS 리전으로 변경합니다.
3. 왼쪽 탐색 창에서 구독을 선택한 다음 구독 생성을 선택합니다.
4. 다음 정보를 제공합니다.
 - a. 주제 ARN: `arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}` 여기서 REGION은 선택한 AWS 리전(SNS 알림이 생성된 리전)이고 AMS_AMI_NAME은 알림을 받을 AMI입니다. 예시:
 - AWS 리전 us-east-1의 새 AMS Amazon Linux AMIs 알림을 구독하려면이 주제 ARN =를 사용합니다`arn:aws:sns:us-east-1:287847593866:customer-ams-amazon1`.
 - AWS 리전 us-west-2의 새 AMS Window Server 2016 AMIs 알림을 구독하려면이 주제 ARN = `arn:aws:sns:us-west-2:287847593866:customer-ams-windows2016`
 - b. 프로토콜에서 이메일을 선택합니다.
 - c. 엔드포인트에 알림 받을 이메일 주소를 입력합니다. 개인의 이메일 대신 배포 목록을 사용하는 것이 좋습니다.
5. 구독 생성을 선택합니다.
6. “AWS 알림 - 구독 확인”이라는 제목의 확인 이메일을 받으면 이메일을 열고 구독 확인을 선택하여 구독을 완료합니다.

 Note

프로토콜에 대한 이메일에만 국한되지 않습니다. 허용되는 다른 프로토콜 및 사용 방법에 대한 자세한 내용은 [구독](#)을 참조하세요.

AWS SNS 콘솔을 사용하여 AMS 새 AMI 알림 구독을 취소하려면:

1. Amazon SNS 콘솔의 [대시보드](#)를 엽니다.
2. 탐색 모음에서 원하는 AWS 리전으로 변경합니다. 해당 AMIs에 대한 알림을 수신하려는 AWS 리전을 사용해야 합니다.
3. 탐색 창에서 구독을 선택하고 구독을 선택한 다음 작업 -> 구독 삭제를 선택합니다.
4. 확인 메시지가 나타나면 삭제를 선택합니다.

배포 | 수집 | CloudFormation 템플릿의 스택 | 생성(ct-36cn2avfrrj9v)을 사용하여 AMS 새 AMI 알림을 구독하려면:

1. AmazonLinuxSubscription을 구독하려면 실행 파라미터 JSON 파일을 생성하고 저장합니다.이 예제에서는 CreateSubscribeAmiParams.json:이라는 이름을 지정합니다.

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "AmazonLinuxSubscription":{
      "Type" : "AWS::SNS::Subscription",
      "Properties": {
        "TopicArn": "arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}",
        "Protocol": "email",
        "Endpoint": "username@yourdomain.com"
      }
    }
  }
}
```

2. 다음 콘텐츠와 함께 RFC 파라미터 JSON 파일을 생성하고 저장합니다.이 예제에서는 CreateSubscribeAmiRfc.json 파일의 이름을 지정합니다.

```
{
  "ChangeTypeId": "ct-36cn2avfrrj9v",
  "ChangeTypeVersion": "1.0",
  "Title": "cfn-ingest-subscribe-ami"
}
```

3. CreateSubscribeAmiRfc 파일과 CreateSubscribeAmiParams 파일을 지정하여 RFC를 생성합니다.

```
aws amscm create-rfc --cli-input-json file://CreateSubscribeAmiRfc.json --  
execution-parameters file://CreateSubscribeAmiParams.json
```

응답에서 새 RFC의 ID를 수신하고 이를 사용하여 RFC를 제출하고 모니터링할 수 있습니다. 제출하기 전까지는 RFC가 편집 상태로 유지되고 시작되지 않습니다.

AMIs. <https://docs.aws.amazon.com/managedservices/latest/ctref/ex-ami-create-col.html>

프로그래밍 방식으로 AMIs. [EC2](#)

서비스 알림

AMS는 다음을 포함하여 계정 또는 리소스에 영향을 미칠 수 있는 작업을 수행해야 하거나 이를 알고 있어야 하는 경우 아웃바운드 서비스 요청 또는 서비스 알림을 보냅니다.

- 인프라 영향: AMS는 인프라에 영향을 미치는 기본 AWS 서비스가 있고 특정 날짜 이전에 조치를 취해야 하거나 중단이 발생할 수 있는 경우 서비스 알림을 보냅니다.
- EC2 하드웨어 문제: AMS는 특정 날짜 이전에 EC2 인스턴스를 재부팅해야 하는 EC2 하드웨어 문제에 대해 서비스 알림을 보내거나 AMS가 인스턴스를 재부팅할 것임을 알려줍니다. 재부팅으로 인해 중단이 발생할 수 있으므로 이 알림은 중요합니다. 인스턴스를 직접 재부팅하려면 적절한 날짜로 응답하거나 ct-09qbhy7kvtxqw로 RFC를 생성해야 합니다. 응답하지 않으면 이와 같은 서비스 알림이 5일 후에 자동으로 종료됩니다.

RFC 상태 변경 알림

AMS는 이메일 및 CloudWatch Events를 통해 RFC 상태 변경에 대한 알림을 제공합니다.

- AMS 콘솔을 통한 이메일: RFC 생성 마법사의 두 번째 페이지에 RFC 상태가 변경될 때 알림을 받을 이메일 주소를 최대 5개까지 추가할 수 있는 옵션이 있습니다.
- CloudWatch Events: 모든 RFC 상태 변경에 대한 알림을 수신하도록 CloudWatch Events에 대해 다양한 규칙과 대상을 구성할 수 있습니다.

이메일 알림

이메일 주소를 추가하여 AMS 콘솔에서 생성하거나 AMS API/CLI를 사용하여 RFC 상태 변경을 수신할 수 있습니다.

AMS 콘솔에서 RFC 생성 마법사의 두 번째 페이지에 있는 이메일 알림 옵션을 사용합니다.

AMS API/CLI에서 RFC의 RFC 파라미터 섹션에 이와 같은 줄을 추가합니다(실행 파라미터 섹션에 줄을 추가하지 마십시오).

```
--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"
```

알림의 동작은 RFC 일정 유형에 따라 달라집니다.

- 예약된 RFCs에 대한 이메일 알림을 수신합니다. 제출됨, 예약됨, InProgress, 완료됨, 거부됨, 취소됨, 자동 거부됨 또는 자동 취소됨.
- ASAP RFCs 제출됨, InProgress, 완료됨, 거부됨, 취소됨, AutoRejected 또는 자동 취소됨과 같은 이메일 알림을 수신합니다.

Note

- 이메일 알림은 다음 주소에서 전송됩니다no-reply@managedservices.amazonaws.com.
- RFC 제목의 특수 문자와 URLs은 보내는 이메일에서 삭제됩니다. 이는 보안 조치입니다.

CloudWatch Events 알림

AMS는 CloudWatch Events를 통해 RFC 상태 변경에 대한 푸시 알림을 제공합니다. 이러한 알림을 받으려면:

1. 알림이 전송될 주제 및 구독을 생성합니다. 원하는 주제의 이름을 지정할 수 있습니다. 이에 대한 자세한 내용은 [SNS 주제 및 구독: 생성을](#) 참조하세요.
2. 관리 | 기타 | 기타 | 변경 유형 생성으로 RFC를 제출하고 RFC 상태 변경 알림 요청에 SNS 주제 및 구독을 포함합니다.

이 기능에 대한 관리 | 기타 | 기타 RFC 요청을 제출할 때 알림을 받는 데 관심이 있는 RFC 상태 변경 사항과 변경 유형을 지정하고 다른 필터를 설정할 수 있습니다. 예를 들어 관리자 액세스 변경 유형이 EventType = RfcSubmitted이고 EventType = RfcUpdated인 경우에만 알림을 받도록 요청할 수 있습니다.

이는 수신할 수 있는 CloudWatch 이벤트 알림의 템플릿입니다(가능한 모든 값 포함).

```
{
  "source ": "aws.managedservices",
  "detail-type": "AMS RFC State Change",
  "detail": {
    "ActionState": "null | AwsActionPending | AwsOperatorAssigned |
CustomerActionPending | NotApplicable | NoActionPending",
    "ActualExecutionTimeRange": {
      "StartTime": "null | Actual Start Time",
      "EndTime": "null | Actual End Time"
    },
    "AutomationStatus": "Automated | Manual",
    "AwsAccountId": "AWS Account ID",
    "AwsApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending
| Rejected | Approved",
    "ChangeTypeId": "Change_Type_ID",
    "ChangeTypeVersion": "Change_Type_Version",
    "CreatedTime": "Created_Time",
    "CustomerApprovalStatus": "null | SubmissionPending | NotRequired |
ApprovalPending | Rejected | Approved",
    "EventType": "RfcActionStateUpdated | RfcApproved | RfcAutoRejected |
RfcCanceled | RfcCompleted | RfcCreated | RfcInProgress | RfcRejected | RfcSubmitted |
RfcUpdated",
    "LastModifiedTime": "Last_Updated_Time",
    "LastSubmittedTime": "null | Last_Submitted_Time",
    "RequestedExecutionTimeRange": {
      "StartTime": "null | Expected_Start_Time",
      "EndTime": "null | Expected_End_Time"
    },
    "RfcId": "RFC_ID",
    "Status": "Editing | PendingApproval | Scheduled | Rejected | Canceled |
ExecutionLock | InProgress | Success | Failure",
    "Title": "Title"
  }
}
```

실제 CloudWatch Events 알림에 표시되는 지원되는 RFC 상태 변경(EventType)은 다음과 같습니다.

- RfcActionStateUpdated(AMS 콘솔 옵션 없음): 나중에 설명하는 상태 중 하나의 RFC가 변경되었습니다.

- RfcApproved(AMS 콘솔 옵션 없음): RFC가 시스템 및/또는 AMS 운영자 검증을 통과했으며 완료가 승인되었습니다.
- RfcAutoRejected(자동 거부됨): RFC가 시스템 검증 또는 AMS 연산자에 실패했으며 거부되었습니다.
- RfcCanceled(취소됨 또는 자동 취소됨): 제출자 또는 AMS 운영자가 RFC를 취소했습니다.
- RfcCompleted(완료됨): UserData를 포함한 RFC 실행 파라미터가 완료되었습니다.
- RfcCreated(AMS 콘솔 옵션 없음): RFC가 성공적으로 생성되었습니다(JSON 및 제출된 파라미터가 유효함).
- RfcInProgress(InProgress): RFC 실행이 아직 진행 중입니다.
- RfcRejected(Rejected): RFC 실패 시스템 또는 AMS 연산자 검증이 거부되었습니다.
- RfcSubmitted(제출됨): RFC가 제출되었으며 시스템 검증을 진행 중입니다.
- RfcUpdated(AMS 콘솔 옵션 없음): AMS 운영자가 RFC를 수동으로 업데이트했습니다.

또한 CloudWatch Events(CWE) 알림을 지원되는 대상 중 하나로 전송하고 이러한 자동 알림을 기반으로 자체 시스템을 구축할 수 있습니다.

- Amazon EC2 인스턴스
- AWS Lambda 함수
- Amazon Kinesis Data Streams의 스트림
- Amazon Data Firehose의 전송 스트림
- Amazon CloudWatch Logs의 로그 그룹
- Amazon ECS 작업
- Systems Manager Run Command
- Systems Manager Automation
- AWS Batch 작업
- Step Functions 상태 시스템
- CodePipeline의 파이프라인
- CodeBuild 프로젝트
- Amazon Inspector 평가 템플릿
- Amazon SNS 주제
- Amazon SQS 대기열

- 기본 제공 대상: EC2 CreateSnapshot API 호출, EC2 RebootInstances API 호출, EC2 StopInstances API 호출 및 EC2 TerminateInstances API 호출.
- 다른 AWS 계정의 기본 이벤트 버스

Note

RFC 상태 변경에 대한 CloudWatch Events 알림을 최대한 전송합니다.

프라이빗 및 퍼블릭 DNS 설정

온보딩 중에 AMS는 관리형 리소스와 AMS 간의 통신을 위한 프라이빗 DNS 서비스를 설정합니다.

AMS Route 53을 사용하면 정보를 퍼블릭 인터넷에 노출하지 않고도 애플리케이션 리소스(웹 서버, 애플리케이션 서버, 데이터베이스 등)의 내부 DNS 이름을 관리할 수 있습니다. 이렇게 하면 보안 계층이 추가되고 DNS 이름을 다른 IP 주소에 매핑하여 기본 리소스에서 보조 리소스(종종 "폴립"이라고 함)로 장애 조치할 수도 있습니다.

배포 | 고급 스택 구성 요소 | DNS(프라이빗) | 생성(ct-0c38gftq56zj6) 또는 배포 | 고급 스택 구성 요소 | DNS(퍼블릭) | 생성(ct-0vzsr2nyraedl)을 사용하여 프라이빗 DNS 리소스를 생성한 후 관리 | 고급 스택 구성 요소 | DNS(프라이빗) | 업데이트(ct-1d55pi44ff21u) 및 관리 | 고급 스택 구성 요소 | DNS(퍼블릭) | 업데이트(ct-1hzofpphabs3i), CTs 사용하여 추가 레코드 세트를 구성하거나 기존 레코드 세트를 업데이트할 수 있습니다. 다중 계정 랜딩 존(MALZ) 계정의 경우 애플리케이션 계정 VPCs에서 생성된 DNS 리소스를 공유 서비스 계정 VPC와 공유하여 AMS AD를 사용하여 중앙 집중식 DNS를 유지할 수 있습니다.

MALZ

다음 그림은 다중 계정 랜딩 존 AMS에 대해 가능한 DNS 구성을 보여줍니다. AMS와 일반적인 고객 네트워크 간의 하이브리드 DNS 설정을 보여줍니다. 고객 네트워크 DNS 서버의 정식 이름 레코드(CNAME)는 AMS FQDN의 CNAME이 A 레코드로 전달된 조건부 전달을 통해 공유 서비스 계정의 AMS AD DNS로 전달합니다.

SALZ

다음 그림은 단일 계정 랜딩 존(SALZ)에 대해 가능한 DNS 구성을 보여줍니다. AMS와 일반적인 고객 네트워크 간의 하이브리드 DNS 설정을 보여줍니다. 고객 네트워크 DNS 서버의 CNAME은 AMS FQDN의 CNAME이 A 레코드로 전달된 조건부 전달을 통해 AMS AD DNS로 전달합니다.

SALZ Route53 DNS

다음 그림은 단일 계정 랜딩 존(SALZ)에 대해 가능한 DNS 구성을 보여줍니다. AMS와 일반적인 고객 네트워크 간의 하이브리드 DNS 설정을 보여줍니다. 고객 네트워크 DNS 서버의 CNAME은 AMS FQDN의 CNAME이 A 레코드로 전달된 조건부 전달을 통해 AMS AD DNS로 전달합니다. 또한 계정의 모든 애플리케이션이 가용성이 가장 높은 계정에서 DNS 확인을 가질 수 있도록 아웃바운드 네트워크 트래픽에 Route53를 활용합니다.

Route53 지원 해결 경로:

- AMS MAD 이름을 확인하려는 인스턴스 --> VPC +2(Route53/AmazonProvidedDNS) --> 조건부 전달자가 평가됨 --> Route53 MAD 조건부 전달자 규칙이 일치함 --> Route53 아웃바운드 해석기 --> 관리형 AD DNS
- 고객 온프레미스 이름을 확인하려는 인스턴스 --> VPC +2(Route53/AmazonProvidedDNS) --> 조건부 전달자가 평가됨 --> Route53 온프레미스 조건부 전달자 규칙이 일치함 --> Route53 아웃바운드 해석기 --> 고객 온프레미스 DNS
- 인터넷 이름을 확인하려는 인스턴스 --> VPC +2(Route53/AmazonProvidedDNS) --> 조건부 전달자 평가됨 --> 일치하는 전달자 없음 --> 인터넷 DNS 서비스

자세한 내용은 [VPC에서 DNS 사용](#) 및 [프라이빗 호스팅 영역 작업을 참조하세요](#).

AMS 송신 트래픽 관리

기본적으로 AMS 프라이빗 및 고객 애플리케이션 서브넷의 대상 CIDR이 0.0.0.0/0인 라우팅에는 NAT(네트워크 주소 변환) 게이트웨이가 대상으로 사용됩니다. AMS 서비스인 TrendMicro 및 패치는 AMS가 서비스를 제공할 수 있고 TrendMicro 및 운영 체제가 업데이트를 받을 수 있도록 인터넷에 대한 외부 액세스 권한이 있어야 하는 구성 요소입니다.

AMS는 다음과 같은 경우에 한해 고객 관리형 송신 디바이스를 통해 송신 트래픽을 인터넷으로 전환하도록 지원합니다.

- 암시적(예: 투명) 프록시 역할을 합니다.

and

- AMS HTTP 및 HTTPS 종속성(이 섹션에 나열됨)을 허용하여 AMS 관리형 인프라를 지속적으로 패치하고 유지 관리할 수 있습니다.

다음은 몇 가지 예시입니다.

- 전송 게이트웨이(TGW)에는 다중 계정 랜딩 존 네트워킹 계정의 AWS Direct Connect 연결을 통해 고객 관리형 온프레미스 방화벽을 가리키는 기본 경로가 있습니다.
- TGW에는 AWS PrivateLink를 활용하는 다중 계정 랜딩 존 송신 VPC의 AWS 엔드포인트를 가리키는 기본 경로가 있으며, 다른 AWS 계정의 고객 관리형 프록시를 가리킵니다.
- TGW에는 다른 AWS 계정의 고객 관리형 방화벽을 가리키는 기본 경로가 있으며, site-to-site VPN 연결은 다중 계정 랜딩 존 TGW에 대한 연결로 사용됩니다.

AMS는 해당 AMS HTTP 및 HTTPS 종속성을 식별했으며 이러한 종속성을 지속적으로 개발하고 구체화합니다. [egressMgmt.zip](#)을 참조하세요. ZIP에는 JSON 파일과 함께 README가 포함되어 있습니다.

Note

- 이 정보는 포괄적이지 않습니다. 일부 필수 외부 사이트는 여기에 나열되지 않습니다.
- 거부 목록 또는 차단 전략에서 이 목록을 사용하지 마십시오.
- 이 목록은 송신 필터링 규칙 세트의 시작점으로 사용되며, 보고 도구를 사용하여 실제 트래픽이 목록에서 분기하는 위치를 정확하게 결정할 것으로 예상됩니다.

송신 트래픽 필터링에 대한 정보를 요청하려면 CSDM에 ams-csdm@amazon.com으로 이메일을 보내세요.

AMS Advanced에 IAM 리소스 배포

AMS는 다음 두 가지 방법으로 다중 계정 랜딩 존(MALZ) 애플리케이션 및 단일 계정 랜딩 존(SALZ) 계정에 IAM 리소스를 배포합니다.

- 자동 IAM 프로비저닝: AMS의 이 기능을 사용하면 운영자 검토 없이 IAM 및 AMS 검증 검사가 자동으로 실행되는 IAM 역할 또는 정책 프로비저닝에 대한 변경 유형을 생성, 업데이트 또는 삭제할 수 있습니다.

관리 | 관리형 계정 | 읽기-쓰기 권한이 있는 AMS 자동 IAM 프로비저닝 | [변경 유형 활성화\(검토 필요\)](#)(ct-1706xvvk6j9hf)를 사용하여이 기능을 명시적으로 활성화해야 합니다. 자세한 내용은 [자동 IAM 프로비저닝 AMS](#)를 참조하세요. AMS 자동 IAM 프로비저닝이 활성화되면 변경 유형 생성, 업데이트 및 삭제에 액세스하여 IAM 리소스를 관리할 수 있습니다.

- 필요한 IAM 변경 유형 검토:이 변경 유형, 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | [개체 또는 정책 생성\(검토 필요\)](#)(ct-3dpg8mdd9jn1r)에는 AMS 운영자 검토가 필요하며, 설명이 필요한 경우 완료하는 데 며칠이 걸릴 수 있습니다.

Note

어떤 방법을 사용하든 IAM 역할은 관련 계정 또는 계정에 프로비저닝되며, 역할이 프로비저닝 된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

자동 IAM 프로비저닝 AMS

AWS Managed Services (AMS)는 AMS Advanced 변경 요청(RFCs) 및 새 변경 유형(CTs)을 사용하는 역할 및 정책을 포함한 IAM 리소스에 대한 자동 검증 및 프로비저닝을 지원합니다. 이전에는 이러한 요청이 반자동 프로세스를 거쳐 대기 시간이 길어지기도 했습니다. 이제 AMS 자동 IAM 프로비저닝을 사용하여 IAM 리소스를 프로비저닝하고 결과를 훨씬 더 빠르게 얻을 수 있습니다.

AMS의 자동 IAM 프로비저닝 작동 방식

자동 IAM 프로비저닝은 IAM 리소스의 변경 사항을 검증하기 위해 IAM의 자동 런타임 검사에 의존합니다. 변경 유형 생성, 업데이트 또는 삭제가 실행될 때 수행되는 이러한 자동 검사는 과도하게 허용적이거나 안전하지 않은 패턴이 있는 IAM 리소스가 계정에 배포되는 것을 방지합니다. 이를 통해 IAM 검토의 엄격성 수준을 팀의 전문 지식과 일치시킬 수 있습니다. 클라우드 서비스를 처음 사용하고 모든 IAM 리소스 변경 사항에 대한 수동 확인이 필요한 팀은 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | [개체 또는 정책 생성\(검토 필요\)](#) (ct-3dpg8mdd9jn1r)과 같은 기존 검토 필수 변경 유형을 사용하는 것이 좋습니다. 환경에 대한 AWS 전문 지식과 제어를 갖춘 팀은 자동 IAM 프로비저닝을 사용하여 배포 속도를 높일 수 있습니다. 이 기능을 사용하여 자동 런타임 검사를 통해 검증을 수행하거나 검증에 성공한 후 IAM 리소스의 검증 및 프로비저닝을 수행할 수 있습니다.

Important

AWS Managed Services 는 특정 권한 및 조건을 가진 IAM 리소스 또는 정책의 생성을 방지하는 검증 [런타임 검사](#) 목록을 사전에 구현했습니다. 이러한 권한 및 조건에 대한 설명

은 [AMS Advanced](#)에서 IAM 리소스 배포를 참조하세요. 자동 변경 유형 [ct-1n9gfnog5x7fl](#), [ct-1e0xmuy1diafq](#) 및 [ct-17cj84y7632o6](#)을 사용하면 IAM 리소스를 관리하는 데 능숙한 사용자가 읽기 전용 권한을 초과하는 작업을 허용하는 IAM 역할 및 정책을 프로비저닝할 수 있습니다.

또한 자동화된 변경 유형 [ct-1n9gfnog5x7fl](#), [ct-1e0xmuy1diafq](#) 및 [ct-17cj84y7632o6](#)을 통해 생성된 역할을 사용하여 새 리소스를 생성할 수 있습니다. 그러나 리소스는 AMS 이름 지정 표준을 따를 수 없으며 표준 AMS 스택의 일부가 아닙니다. AMS는 최선을 다해 특정 리소스의 운영 및 보안 지원을 제공합니다.

수동 프로세스와 자동 프로세스 모두 보안 표준을 준수하는 것을 목표로 하지만 두 프로세스 간의 점검에는 차이가 있다는 점에 유의해야 합니다. 자동 프로비저닝을 사용하면 역할 및 정책을 생성하고 업데이트할 수 있는 유연성이 향상되므로 역할 및 정책이 동일하지 않습니다. 조직에서 AMS 사용 설명서에 나열된 검증 [런타임 검사](#)를 주의 깊게 검토하여 조직의 기대치 및 요구 사항에 부합하는지 확인하는 것이 좋습니다.

검증 흐름

검증 및 프로비저닝 흐름

Note

이 기능은 AWS 및 IAM 리소스 경험이 있는 팀에 적합하며, 처음 사용하는 팀에는 권장하지 않습니다. AWS. 자동 검증 프로세스는 대부분의 오류를 포착하도록 설계되었으며 팀이 필요한 권한을 이해할 때 IAM 변경 사항에 대한 빠른 검토를 받는 데 유용합니다. 새로운 변경 유형을 안전하고 효과적으로 사용하려면 AWS IAM과 변경 유형이 제공하는 [런타임 검사](#)를 잘 이해하여 팀에 적합한지 확인하는 것이 좋습니다.

AMS에서 AMS 자동 IAM 프로비저닝에 온보딩

새 변경 유형을 사용하려면 먼저 관리 | 관리형 계정 | 읽기-쓰기 권한이 있는 AMS 자동 IAM 프로비저닝 | [활성화\(검토 필요\)](#)(ct-1706xvvk6j9hf)와 같은 변경 유형을 사용하여 RFC를 제출하여 AMS 자동 IAM 프로비저닝을 활성화합니다. AWS에서는 이러한 변경 유형의 사용이 조직 정책에 부합하는지 확인하기 위해 조직이 고객 보안 위험 관리(CSRM) 프로세스를 거쳐야 합니다. AWS 운영 팀은 고객과 협력하여 필수 검토의 일환으로 위험 수락의 형태로 보안 팀 연락처로부터 명시적 승인을 받습니다. 자세한 내용은 [RFC 고객 위험 관리\(CSRM\) 프로세스](#)를 참조하세요.

읽기-쓰기 권한 기능을 사용하여 AMS 자동 IAM 프로비저닝을 켜기 위한 RFC가 성공하면 AMS는 활성화 RFC를 제출하는 데 사용되는 계정에서 AMS 자동 IAM 프로비저닝 변경 유형을 활성화합니다. 계정에 AMS 자동 IAM 프로비저닝이 켜져 있는지 확인하려면 IAM 콘솔에서 `AWSManagedServicesIAMProvisionAdminRole` 역할을 확인합니다.

온보딩의 일환으로 AMS는 계정의 동일한 AWS 리전에 IAM Access Analyzer를 프로비저닝하여 액세스 미리 보기 기능을 활용합니다. IAM Access Analyzer는 외부 엔터티와 공유되는 조직 및 계정의 리소스를 식별하고, 정책 문법 및 모범 사례를 기준으로 IAM 정책을 검증하고, AWS CloudTrail 로그의 액세스 활동을 기반으로 IAM 정책을 생성하는 데 도움이 됩니다. 자세한 내용은 [사용을 AWS Identity and Access Management Access Analyzer](#) 참조하세요.

온보딩되면 `AWSManagedServicesIAMProvisionAdminRole`가 활성화된 계정에 배포됩니다. SAML 페더레이션을 통해 이 역할을 사용하기로 선택한 경우 해당 역할을 페더레이션 솔루션에 온보딩해야 합니다.

온보딩의 일환으로 `AWSManagedServicesIAMProvisionAdminRole`의 신뢰 정책을 업데이트하여 사용하여 이 역할을 수임할 다른 IAM 역할 ARN을 부여하도록 요청할 수 있습니다 AWS Security Token Service.

AMS에서 AMS 자동 IAM 프로비저닝 사용

다음 AMS 자동 IAM 프로비저닝 변경 유형을 사용하여 RFCs를 생성할 수 있습니다.

Note

- 역할 및 정책에 대한 프로비저닝만 지원됩니다.

역할을 업데이트하는 동안 CT 업데이트는 관리형 정책 Amazon 리소스 이름(ARNs)의 기존 목록과 "역할 수임" 정책 문서를 제공된 관리형 정책 ARNs 및 "역할 수임" 정책 문서로 대체합니다. 예를 들어 기존 관리형 정책 ARN 목록에서 ARNs를 추가하거나 제거하는 경우 "역할 수임" 정책 문서에 개별 정책 설명을 추가하거나 제거하는 것은 허용되지 않습니다. 마찬가지로 정책을 업데이트하는 동안 CT 업데이트는 기존 정책 문서를 대체하며 기존 정책 문서에서 개별 정책 설명을 추가하거나 제거하는 것을 허용하지 않습니다.

- “검증 전용” 옵션을 선택하면 IAM 엔터티 또는 정책을 프로비저닝하지 않고 런타임 검사가 수행됩니다. 조사 결과에 관계없이 RFC 상태는 “성공”입니다. “성공” 상태는 제공된 IAM 엔터티 또는 정책에 대한 검증이 성공했음을 나타냅니다.

- 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | [엔터티 또는 정책 생성\(읽기-쓰기 권한\)](#)(ct-1n9gfnog5x7fl): 새 IAM 엔터티 또는 정책이 자동으로 검증되고 프로비저닝됩니다.
- 관리 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | [엔터티 또는 정책 업데이트\(읽기-쓰기 권한\)](#)(ct-1e0xmuy1diafq): 기존 IAM 엔터티 또는 정책이 자동으로 업데이트되고 검증됩니다.
- 관리 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | [엔터티 또는 정책 삭제\(읽기-쓰기 권한\)](#)(ct-17cj84y7632o6): 자동 엔터티 생성 또는 정책 변경 유형을 사용하여 프로비저닝된 기존 IAM 엔터티 또는 정책이 삭제됩니다.

전용 IAM 역할인을 사용하여 앞의 세 CTs만 호출할 수 있습니다

다AWSManagedServicesIAMProvisionAdminRole. 이 역할은 관리 | 관리형 계정 | AMS 자동 IAM 프로비저닝 읽기-쓰기 권한 | [활성화\(검토 필요\)](#)(ct-1706xvvk6j9hf)를 사용하여 기능에 온보딩된 계정에 서만 사용할 수 있습니다.

Important

변경 유형 생성, 업데이트 및 삭제는 항상 계정에 표시되지만 기본적으로 켜져 있지는 않습니다. AMS 자동 IAM 프로비저닝 기능을 먼저 활성화하지 않고 이러한 변경 유형 중 하나를 사용하여 RFC를 제출하려고 하면 "무단" 오류가 표시됩니다.

제한:

- CT 생성을 통해 AWS 리소스를 생성할 권한이 있는 IAM 역할 또는 정책을 생성할 수 있습니다. 그러나 이러한 역할 및 정책으로 생성된 AWS 리소스는 AMS에서 관리하지 않습니다. 이러한 역할 또는 정책의 생성을 제한하기 위해 조직의 통제를 준수하는 것이 가장 좋습니다.
- CT 업데이트는 CFN Ingest, Direct Change Mode, Developer Mode 또는 경우에 따라 기존 AMS Advanced 수동 또는 자동 CTs를 통해 생성된 IAM 역할 및 정책을 수정할 수 없습니다.
- CT 삭제는 AMS 자동 IAM 프로비저닝 CT 생성으로 생성되지 않은 기존 역할 또는 정책을 삭제할 수 없습니다.
- 읽기-쓰기 권한이 있는 AMS 자동 IAM 프로비저닝 기능은 직접 변경 모드 역할에서 지원되지 않습니다. 즉, 이러한 역할을 사용하여 읽기-쓰기 권한으로 IAM 역할 및 정책을 프로비저닝하거나 업데이트할 수 없습니다.
- 읽기-쓰기 권한이 있는 AMS 자동 IAM 프로비저닝 변경 유형 생성, 업데이트 및 삭제는 ServiceNow 커넥터와 호환되지 않습니다.

AMS에서 AMS 자동 IAM 프로비저닝에 대한 런타임 확인

자동 IAM 프로비저닝은 AMS 경계 정책의 검사를 활용하고 AMS 경계 정책에 대해 추가 검사 및 검증을 AWS Identity and Access Management Access Analyzer수행합니다. AMS는 IAM 모범 사례, 클라우드에서 고객 워크로드 운영 경험, 집합 AMS IAM 수동 평가 경험을 기반으로 추가 확인 및 검증을 정의했습니다.

변경 요청(RFC) 출력에서 정책 런타임 검사 결과를 볼 수 있습니다. 조사 결과에는 리소스 식별자, 조사 결과를 생성한 역할 및/또는 정책 내 위치, IAM 엔터티 또는 리소스가 통과하지 못했는지 확인하는 메시지가 포함됩니다. 이러한 결과는 제대로 작동하고 보안 모범 사례를 준수하는 정책을 작성하는 데 도움이 됩니다.

Note

자동 IAM 프로비저닝은 검사를 통과하지 못하는 엔터티 또는 정책 정의 내의 위치에 대해 특정하려고 시도합니다. 유형에 따라 위치에 리소스 이름이나 ARN 또는 배열 내의 인덱스가 포함될 수 있습니다. 예를 들어, 성공적인 결과를 위해 엔터티 또는 정책을 조정하는 데 도움이 되는 문입니다.

원활한 AMS 자동 IAM 프로비저닝 환경을 위해 RFC 출력에 보고된 검증 검사 결과가 없을 때까지 “검증 전용” 옵션을 사용하여 검증 검사를 실행하는 것이 좋습니다. 검증 검사에서 결과가 보고되지 않으면 AMS 콘솔에서 복사본 생성을 선택하여 기존 RFC의 복사본을 빠르게 생성합니다. 프로비저닝할 준비가 되면 파라미터 섹션에서 유효성 검사 전용 값을 예에서 아니요로 전환한 다음 계속 진행합니다.

다음은 IAM 리소스가 안전한지 확인하기 위해 AMS 자동 IAM 프로비저닝이 수행하는 런타임 검사입니다.

Note

이러한 자동 변경 유형에서 거부한 작업이 포함된 IAM 정책을 프로비저닝하려면 RFC 고객 보안 위험 관리(CSRM) 프로세스를 따라야 합니다. 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 개체 또는 정책 생성(검토 필요)(ct-3dpd8mdd9jn1r) 변경 유형을 사용합니다.

- IAM Access Analyzer 정책 확인 및 검증: [Access Analyzer 정책 확인 참조](#) 및 [IAM Access Analyzer 정책 검증](#)도 참조하세요.

- AMS 권한 경계 정책 검사: 기본적으로 거부되는 서비스 세트에 대한 작업입니다. 자세한 내용은 [자동 IAM 프로비저닝 권한 경계 검사를 참조하세요](#).
- 고객 정의 권한 경계 정책 검사: 거부된 서비스 세트에 대한 추가 제한 작업입니다. 자세한 내용은 [자동 IAM 프로비저닝 권한 경계 검사를 참조하세요](#).
- AMS 정의 사용자 지정 검사: 요청된 IAM 엔터티 또는 정책 내에서 다양한 안전하지 않고 지나치게 허용적인 정책 또는 액세스 패턴을 식별하는 검사이며 요청이 발견되면 요청을 거부합니다. 자세한 내용은 [AWS JSON 정책 요소: 보안 주체](#)를 참조하세요.

조사 결과	설명
신뢰 영역 외부에 있는 외부 계정에서 역할에 액세스할 수 있습니다.	이 결과는 신뢰 영역 외부에 있는 역할 신뢰 정책에 나열된 보안 주체를 나타냅니다. 신뢰 영역은 역할이 생성되는 계정 또는 계정이 속한 AWS 조직으로 정의됩니다. 계정 또는 동일한 AWS 조직에 속하지 않는 엔터티는 외부 엔터티입니다. 조사 결과를 해결하려면 보안 주체 ARNs의 계정 ID를 검토하고 해당 ID가 사용자에게 속하고 AMS 온보딩 계정인지 확인합니다.
역할은 AMS 고객 소유 계정 Account_ID# ### # ## External_Account_ID# ### # ##### # ##.	이 결과는 역할 신뢰 정책에 사용자가 소유하지 않은 계정 ID가 있는 보안 주체 ARN과 AMS 온보딩 계정이 포함된 경우 생성됩니다. 이 결과를 해결하려면 역할 신뢰 정책에서 해당 보안 주체를 제거합니다.
정식 사용자 ID는 IAM 신뢰 정책에서 지원되는 보안 주체가 아닙니다.	정식 보안 주체 IDs는 IAM 신뢰 정책에서 지원되지 않습니다. 조사 결과를 해결하려면 역할 신뢰 정책에서 해당 보안 주체를 제거합니다.
신뢰 영역 외부에 있는 외부 웹 자격 증명에서 역할에 액세스할 수 있습니다.	이 결과는 역할 신뢰 정책이 SAML IdP 이외의 외부 웹 자격 증명 공급자(IdP)를 허용하는 경우 생성됩니다. 이 결과를 해결하려면 역할 신뢰 정책을 검토하고 sts:AssumeRoleWithWebIdentity 작업을 허용하는 문을 제거합니다.

조사 결과	설명
역할은 SAML 페더레이션을 통해 액세스할 수 있지만 제공된 SAML ID 제공업체(IdP)는 존재하지 않습니다.	이 결과는 역할 신뢰 정책에 계정에 없는 SAML IdP가 포함된 경우 생성됩니다. 문제를 해결하려면 나열된 모든 SAML IdP가 계정에 있어야 합니다.
정책에는 관리자 또는 고급 사용자 액세스와 동등한 권한이 있는 작업이 포함되어 있습니다. 권한 범위를 특정 서비스, 작업 또는 리소스로 줄이는 것이 좋습니다. NotAction 또는 NotResource와 같은 고급 정책 요소를 사용하는 경우 특히 Allow 문에서 의도한 것보다 더 많은 액세스 권한을 부여하지 않는지 확인합니다.	IAM 정책 AWS Identity and Access Management 으로 권한을 설정할 때 작업을 수행하는 데 필요한 권한만 부여하는 것의 모범 보안 사례입니다. 최소 권한 권한이라고도 하는 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의하여 작업을 수행합니다. 이 결과는 자동화가 정책을 감지하여 광범위한 권한을 부여하고 최소 권한 원칙을 준수하지 않을 때 생성됩니다. 조사 결과를 해결하려면 권한을 검토하고 줄입니다.
문에는 <i>Service_Name</i> 에 대한 권한이 있는 작업이 포함되어 있습니다. 거부 문을 사용하여 이러한 작업을 제외하는 것이 좋습니다. 권한 있는 작업 목록은 AMS 설명서의 경계 정책 참조를 참조하세요.	AMS는 특정 서비스에 대한 특정 작업을 위험한 것으로 식별했으며 고객 보안 팀의 추가 위험 검토 및 수락이 필요합니다. 이 결과는 자동화가 해당 권한을 부여하는 지정된 정책을 감지할 때 생성됩니다. 이 결과를 해결하려면 정책에서 이러한 작업을 거부합니다. 작업 목록은 AMS 경계 정책을 참조하세요. AMS 경계 정책에 대한 자세한 내용은 섹션을 참조하세요 AMS 자동 IAM 프로비저닝 권한 경계 확인.
문은 <i>Service_Name</i> 에 대한 권한 있는 RFC 변경 유형인 ct-1n9gfnog5x7fl, ct-1e0xmu y1diafq 및 ct-17cj84y7632o6에 대한 액세스 권한을 부여합니다. 권한 범위를 특정 변경 유형으로 조정하거나 거부 문을 사용하여 이러한 변경 유형을 제외하는 것이 좋습니다.	이 결과는 정책이 자동 IAM 프로비저닝 변경 유형(CTs)을 사용하여 RFC 관련 작업을 수행할 수 있는 권한을 부여하는 경우에 생성됩니다. CTs는 위험 승인을 받아야 하며 온보딩된 역할을 통해서만 사용해야 합니다. 따라서 이러한 CTs에는 권한을 부여할 수 없습니다. 이 결과를 해결하려면 이러한 CTs.

조사 결과	설명
문에는 Service_Name 서비스에 대한 리소스로 범위가 지정되지 않은 권한이 있는 작업이 포함되어 있습니다. 작업을 특정 리소스로 범위를 조정하거나 AMS 네임스페이스 접두사가 있는 리소스를 제외하는 것이 좋습니다. 와일드카드를 사용하는 경우 범위를 리소스로 제한해야 합니다.	이 결과는 정책이 지정된 서비스의 리소스로 범위가 지정되지 않은 권한 있는 작업을 부여하는 경우에 생성됩니다. 와일드카드는 광범위한 리소스 또는 작업을 권한 범위로 가져오는 지나치게 허용적인 정책을 생성하는 경우가 많습니다. 조사 결과를 해결하려면 소유한 리소스에 대한 권한 범위를 줄이거나 AMS 네임스페이스에 있는 리소스를 제외합니다. AMS 네임스페이스 접두사 목록은 AMS 설명서의 경계 정책을 참조하세요. 모든 접두사가 모든 서비스에 적용되는 것은 아닙니다. AMS 경계 정책에 대한 자세한 내용은 섹션을 참조하세요 AMS 자동 IAM 프로비저닝 권한 경계 확인.
잘못된 계정 ID 또는 Amazon 리소스 이름 (ARN).	이 결과는 정책 또는 역할 신뢰 정책에 지정된 ARN 또는 계정 ID가 유효하지 않은 경우 생성됩니다. 서비스에 대한 유효한 리소스 ARN의 리소스를 검토하려면 서비스 승인 참조를 참조하세요. 계정 ID가 12자리 숫자이고 계정이 활성 상태인지 확인합니다 AWS.
ARN의 계정 ID에 와일드카드(*)를 사용하는 것은 제한됩니다.	이 결과는 ARN의 계정 ID 필드에 와일드카드(*)가 지정된 경우 생성됩니다. 계정 ID 필드의 와일드카드는 모든 계정과 일치하며 잠재적으로 리소스에 의도하지 않은 권한을 부여합니다. 이 문제를 해결하려면 와일드카드를 특정 계정 ID로 바꿉니다.
동일한 AMS 고객 소유 Account_ID가 소유하지 않은 지정된 리소스 계정입니다.	이 결과는 리소스 ARN에 지정된 계정 ID가 사용자에게 속하지 않고 AMS에서 관리하지 않는 경우에 생성됩니다. 이 문제를 해결하려면 모든 리소스(정책에서 ARN으로 지정됨)가 AMS에서 관리하는 계정에 속하는지 확인합니다.

조사 결과	설명
역할 이름은 AMS 제한 네임스페이스에 있습니다.	이 결과는 AMS 예약 접두사로 시작하는 이름으로 역할을 생성하려고 할 때 생성됩니다. 이 문제를 해결하려면 사용 사례에 맞는 역할 이름을 사용합니다. AMS 예약 접두사 목록은 AMS 예약 접두사를 참조하세요 .
정책 이름은 AMS 제한 네임스페이스에 있습니다.	이 결과는 AMS 예약 접두사로 시작하는 이름으로 정책을 생성하려고 할 때 생성됩니다. 이 문제를 해결하려면 사용 사례에 맞는 정책의 이름을 사용합니다. AMS 예약 접두사 목록은 AMS 예약 접두사를 참조하세요 .
ARN의 리소스 ID는 AMS 제한 네임스페이스에 있습니다.	이 결과는 AMS 네임스페이스에 있는 명명된 리소스에 권한을 부여하는 정책을 생성하려고 할 때 생성됩니다. 이 문제를 해결하려면 리소스에 대한 권한의 범위를 지정하거나 AMS 네임스페이스에 있는 리소스에 대한 권한을 거부해야 합니다. AMS 네임스페이스에 대한 자세한 내용은 AMS 제한된 네임스페이스를 참조하세요 .
정책 변수 대/소문자가 잘못되었습니다. 변수를 <i>Variable_Names</i> 로 업데이트합니다.	이 결과는 잘못된 경우 IAM 글로벌 정책 변수가 포함된 정책을 생성하려고 할 때 생성됩니다. 이 문제를 해결하려면 정책의 글로벌 변수에 올바른 사례를 사용합니다. 전역 변수 목록은 AWS 전역 조건 컨텍스트 키를 참조하세요 . 정책 변수에 대한 자세한 내용은 IAM 정책 요소: 변수 및 태그를 참조하세요 .
문에는 KMS 키로 범위가 지정되지 않은 권한이 있는 작업이 포함되어 있습니다. 이러한 권한을 특정 키로 조정하거나 AMS 소유 키를 제외하는 것이 좋습니다.	이 결과는 정책에 소유한 특정 KMS 키로 범위가 지정되지 않은 권한이 포함된 경우 생성됩니다. 이 문제를 해결하려면 권한 범위를 특정 키로 지정하거나 AMS 소유의 키를 제외합니다. AMS 소유 키에는 특정 별칭 세트가 있습니다. AMS 소유 키 별칭 목록은 섹션을 참조하세요 AMS 자동 IAM 프로비저닝 권한 경계 확인 .

조사 결과	설명
문에는 KMS 키 별칭으로 범위가 지정되지 않은 권한이 있는 작업이 포함되어 있습니다. 이러한 권한을 키 또는 별칭으로 조정하거나 AMS 소유 키 별칭을 제외하는 것이 좋습니다.	이 결과는 소유한 특정 KMS 키 별칭으로 범위가 지정되지 않은 권한이 정책에 포함된 경우 생성됩니다. 이 문제를 해결하려면 권한 범위를 특정 키로 지정하거나 AMS 소유의 키를 제외합니다. AMS 소유 키에는 특정 별칭 세트가 있습니다. AMS 소유 키 별칭 목록은 섹션을 참조하세요 AMS 자동 IAM 프로비저닝 권한 경계 확인.
문에는를 사용하여 KMS 키로 범위가 적절하게 지정되지 않은 권한이 있는 작업이 포함되어 있습니다 <code>kms:ResourceAliasesCondition</code> . 조건 키에 적절한 집합 연산자와 함께 특정 별칭 이름을 사용하는 것이 좋습니다. 별칭 이름에 와일드카드를 사용하는 경우 범위를 제한된 KMS 키 세트로 제한해야 합니다.	이 결과는 조건을 사용하고를 사용하여 KMS 키의 별칭으로 범위를 좁히지 않고 KMS 키에 대한 권한을 조정 <code>kms:ResourceAliases</code> 하는 경우에 생성됩니다. 또는 <code>kms:ResourceAliases</code> 조건 키에 AMS 소유 KMS 키 별칭도 포함하는 값이 있는 경우. 이 문제를 해결하려면 KMS 키의 별칭으로만 권한 범위를 좁히거나 AMS 소유 KMS 키의 별칭을 제외하도록 조건을 업데이트합니다. AMS 소유 키 별칭 목록은 섹션을 참조하세요 AMS 자동 IAM 프로비저닝 권한 경계 확인.
역할에 <code>customer_deny_policy</code>가 연결되어 있어야 합니다. 관리형 정책 ARN 목록에 정책 ARNs 포함합니다.	이 결과는 생성 중인 역할에이 <code>customer_deny_policy</code> 연결되어 있지 않은 경우 생성됩니다. 이 문제를 해결하려면 관리형 정책 ARNs 목록에 <code>customer_deny_policy</code> 를 포함합니다.
AWS 관리형 정책은 지나치게 허용적이거나 AMS 경계 정책에 의해 제한된 권한을 부여합니다.	이 결과는 역할의 <code>ManagedPolicyArns</code> 값에 관련 서비스에 대한 전체 또는 관리자 수준 액세스를 제공하는 AMS 관리형 정책이 포함된 경우 생성됩니다. 이를 해결하려면 AWS 관리형 정책의 사용을 검토하고 범위 축소 권한을 제공하는 정책을 사용하거나 최소 권한 원칙을 따르는 자체 정책을 정의합니다.

조사 결과	설명
고객 관리형 정책은 제한된 AMS 네임스페이스에 있습니다.	이 결과는 AWS 네임스페이스에 이름이 접두사로 지정된 고객 관리형 정책이 역할에 연결된 경우 생성됩니다. 이 문제를 해결하려면 역할의 ManagedPolicyArn 목록에서 정책을 제거합니다.
customer_deny_policy는 역할에서 분리할 수 없습니다. 관리형 정책 ARN 목록에 정책 ARNs 포함합니다.	이 결과는 업데이트 중에 customer_deny_policy 가 역할에서 분리된 경우 생성됩니다. 이 문제를 해결하려면 역할의 customer_deny_policy ManagedPolicyArns 필드에를 추가하고 다시 시도하세요.
고객 관리형 정책은 AMS Change Management 서비스 외부 또는 사전 검증 없이 프로비저닝되었습니다.	이 결과는 하나 이상의 기존 고객 관리형 정책 ARNs이 역할에 연결되어 있고 정책이 AMS Change Management 서비스(RFC를 통해)를 통해 프로비저닝되지 않은 경우 생성됩니다. 예를 들어 개발자 모드 또는 직접 변경 모드를 사용하면 고객이 RFC 없이 IAM 정책을 프로비저닝할 수 있습니다. 이 문제를 해결하려면 역할의 ManagedPolicyArns 목록에서 고객 관리형 정책 ARNs을 제거합니다.
제공된 관리형 정책 ARNs 초과합니다.	이 결과는 역할에 연결된 총 관리형 정책 수가 역할 할당량당 정책을 초과하는 경우 생성됩니다. IAM 할당량에 대한 자세한 내용은 IAM 및 AWS STS 할당량, 이름 요구 사항 및 문자 제한을 참조하세요 . 이 정보를 사용하여 역할에 연결하는 정책 수를 줄입니다.
신뢰 정책 크기({trust_policy})가 {size}의 수임 역할 정책 크기 할당량을 초과합니다.	이 결과는 역할 수임 정책 문서의 크기가 정책 크기 할당량을 초과하는 경우 생성됩니다. IAM 할당량에 대한 자세한 내용은 IAM 및 AWS STS 할당량, 이름 요구 사항 및 문자 제한을 참조하세요 .

조사 결과	설명
문에는 Amazon S3에 대한 모든 변형 작업이 포함되어 있습니다. 이러한 권한을 필요한 작업으로만 조정하는 것이 좋습니다. 와일드카드를 사용하는 경우 제한된 변형 작업 집합의 범위를 지정해야 합니다.	이 결과는 지정된 정책이 하나 이상의 리소스에 관계없이 모든 Amazon Simple Storage Service 변형 권한을 부여하는 경우 생성됩니다. 이 문제를 해결하려면 버킷에 대해 필요한 Amazon S3 변형 작업만 포함합니다.
문에는 Amazon S3의 버킷에 대해 허용되지 않는 권한이 있는 작업이 포함되어 있습니다. 이러한 작업을 거부하는 문을 추가하는 것이 좋습니다.	이 결과는 정책이 버킷에 대한 권한 있는 작업을 부여하는 경우에 생성됩니다. 권한 있는 작업 목록은 정책에서이 결과 AMS 자동 IAM 프로비저닝 권한 경계 확인 해결, 제거 또는 거부를 참조하세요.
문에는 Amazon S3의 버킷으로 범위가 지정되지 않은 권한이 있는 작업이 포함되어 있습니다. 버킷을 포함하거나 AMS 네임스페이스 접두사가 있는 버킷을 제외하는 것이 좋습니다. 와일드카드를 사용하는 경우 네임스페이스 내의 버킷과 일치하는지 확인합니다.	이 결과는 정책이 버킷에만 범위가 지정되지 않은 Amazon S3 작업을 부여하는 경우에 생성됩니다. 이는 버킷 리소스를 지정할 때 와일드카드를 사용하는 경우에 자주 발생합니다. 이 문제를 해결하려면 소유한 버킷 이름 또는 ARNs 지정하거나 AMS 네임스페이스 접두사가 있는 버킷을 제외합니다.
문에는 Amazon S3의 버킷으로 범위가 지정되지 않은 권한이 있는 작업이 포함되어 있습니다. 계정의 모든 버킷 범위를 지정하는 와일드카드(*)를 사용하지 않는 것이 좋습니다.	이 결과는 정책이 버킷으로 범위가 지정되지 않은 Amazon S3 작업을 부여하는 경우에 생성됩니다. 이는 버킷 리소스를 지정할 때 와일드카드를 사용하는 경우에 자주 발생합니다. 이 문제를 해결하려면 소유한 버킷 이름 또는 ARNs 지정하거나 AMS 네임스페이스 접두사가 있는 버킷을 제외합니다.

조사 결과	설명
문에는 존재하지 않는 버킷 및 소유하지 않은 버킷을 포함하여 모든 Amazon S3 버킷으로 범위가 지정된 리소스 와일드카드가 포함되어 있습니다. 조건 및 <code>s3:ResourceAccount</code> 조건 키를 사용하여 권한 범위를 조정하는 것이 좋습니다.	이 결과는 정책이 와일드카드를 사용하여 지정된 버킷에 권한을 부여하는 경우 생성됩니다. 와일드카드를 사용하면 기존에 존재하지 않거나 소유하지 않은 버킷의 범위가 지정되는 경우가 많습니다. 이 문제를 해결하려면 조건과 <code>aws:ResourceAccount</code> 조건 키를 사용하여 현재 계정 내의 버킷에만 권한 범위를 지정합니다. 자세한 내용은 특정 AWS 계정이 소유한 Amazon S3 버킷에 대한 액세스 제한을 참조하세요.
문에는 <code>NotResource</code> 정책 요소가 포함되어 있으며, 이 요소는 존재하지 않는 버킷과 소유하지 않은 버킷을 포함하여 많은 수의 버킷으로 범위가 지정될 수 있습니다. 조건 및 <code>s3:ResourceAccount</code> 조건 키를 사용하여 권한 범위를 조정하는 것이 좋습니다.	이 결과는 정책이 <code>NotResources</code> 정책 요소를 활용하여 버킷 리소스를 지정하는 경우 생성됩니다. <code>NotResource</code> 요소를 사용하면 존재하지 않거나 소유하지 않은 버킷을 포함하여 많은 수의 버킷의 범위가 지정될 수 있습니다. 이 문제를 해결하려면 조건과 <code>aws:ResourceAccount</code> 조건 키를 사용하여 현재 계정 내의 버킷에만 권한 범위를 지정합니다.
문에는 존재하지 않거나 계정 <code>Account_ID# ### ## Bucket_Name</code>에 대한 Amazon S3 작업이 포함되어 있거나, 이름에 존재하지 않는 버킷 및 소유하지 않은 버킷을 포함하여 많은 수의 버킷으로 범위가 지정될 수 있는 와일드카드가 포함되어 있습니다. 조건 및 조건 <code>s3:ResourceAccount</code> 키를 사용하여 권한 범위 조정 고려	이 결과는 정책이 존재하지 않거나, 사용자가 소유하지 않거나, 많은 수의 버킷을 포함하는 버킷 이름에 와일드카드가 있고 액세스 범위가 현재 계정으로만 지정되지 않은 버킷에 권한을 부여하는 경우에 생성됩니다. 이 문제를 해결하려면 조건과 <code>aws:ResourceAccount</code> 조건 키를 사용하여 현재 계정 내의 버킷에만 권한 범위를 지정합니다.

조사 결과	설명
문에는 존재하지 않거나 <code>Account_ID# #### ## ## Bucket_Name</code>에 대한 Amazon S3 작업이 포함되어 있거나, 이름에 존재하지 않는 버킷 및 소유하지 않은 버킷을 포함하여 많은 수의 버킷으로 범위가 지정될 수 있는 와일드카드가 포함되어 있습니다. 조건에서 <code>s3:ResourceAccount</code> 또는 지정된 리소스 계정을 사용하여 액세스를 제한하지 않으며, 이는 사용자에게 속하지 않습니다.	이 결과는 정책이 존재하지 않거나, 사용자가 소유하지 않거나, 많은 수의 버킷을 포함하는 버킷 이름에 와일드카드가 있고 액세스 범위가 특정 계정으로만 지정된 버킷에 권한을 부여하는 경우에 생성됩니다. 그러나 <code>aws:ResourceAccount</code> 조건 키에 지정된 계정은 사용자에게 속하지 않으며 AMS에서 관리합니다. 이 문제를 해결하려면 <code>aws:ResourceAccount</code> 조건 키를 업데이트하고 소유하며 AMS에서 관리하는 적절한 계정 ID를 설정합니다.
문에는 Amazon EC2용 인스턴스로 범위가 지정되지 않은 권한이 있는 작업이 포함되어 있습니다. 작업을 특정 인스턴스 ARNs으로 범위를 조정하거나 AMS 네임스페이스 접두사에 값이 있는 이름 태그 키가 있는 인스턴스를 제외하는 것이 좋습니다. 와일드카드를 사용하는 경우 소유한 네임스페이스와 일치하는지 확인합니다.	이 결과는 정책이 AMS가 소유한 Amazon EC2 인스턴스에 대한 권한 있는 작업을 부여하는 경우에 생성됩니다. AMS 인스턴스에는 AMS 네임스페이스의 값이 있는 이름 태그 키로 태그가 지정됩니다. 이 문제를 해결하려면 리소스를 지정하거나 <code>StringNotLike</code> 연산자를 사용하여 AMS 네임스페이스의 값을 제외하는 <code>aws:ResourceTag/Name</code> 키가 있는 조건으로 AMS 인스턴스를 제외합니다.
문에는 AWS Systems Manager 파라미터 스토어의 리소스로 범위가 지정되지 않은 권한이 있는 작업이 포함되어 있습니다. 파라미터의 ARNs을 지정하거나 AMS 네임스페이스 접두사가 있는 파라미터를 제외하는 것이 좋습니다. 와일드카드를 사용하는 경우 파라미터의 범위만 지정해야 합니다.	이 결과는 정책이 소유하지 않은 파라미터에 권한을 부여하는 경우 생성됩니다. 이는 일반적으로 와일드카드를 사용하거나 AMS 네임스페이스 접두사가 있는 파라미터가 정책 설명의 리소스 아래에 나열되는 경우입니다. 이 문제를 해결하려면 네임스페이스 내에 있는 파라미터를 지정하거나 거부 문으로 AMS 파라미터를 제외합니다.
문에는의 리소스에 대한 권한이 있는 작업이 포함되어 있습니다 AWS Systems Manager. 리소스에 대한 작업만 읽을 수 있도록 권한 범위를 조정하는 것이 좋습니다.	이 결과는 정책이 Systems Manager 리소스에 대한 파라미터 스토어 또는 읽기 전용 작업 이외의 권한을 부여하는 경우 생성됩니다. 이 결과를 해결하려면 읽기 전용 작업 또는 파라미터 스토어에 대한 권한만 줄입니다.

조사 결과	설명
문에는 소유한 <i>Service_Name</i> 의 {message} 로 범위가 지정되지 않은 권한이 있는 작업이 포함되어 있습니다. 이러한 권한을 특정 리소스 유형으로 적절하게 조정하거나 AMS 소유 리소스를 제외하는 것이 좋습니다. 와일드카드를 사용하는 경우 <i>###</i>와 일치하는지 확인합니다. 문에는 이름 태그 키의 특정 값으로 범위가 지정되지 않은 {<i>Service_Name</i> }의 태그 지정 작업이 포함되어 있습니다. 네임스페이스의 값으로 <code>aws:RequestTag/Name</code> 조건 키를 설정하여 이러한 작업의 범위를 조정하거나 AMS 네임스페이스 접두사에 값이 있는 StringNot Like 연산자로 <code>aws:RequestTag/Name</code> 조건 키를 설정하여 이러한 작업을 제한하는 것이 좋습니다.	이 결과는 정책이 리소스, 특히 명명된 리소스에 대해 부여되지 않은 권한 있는 작업을 허용하는 경우 생성됩니다. 이 결과를 해결하려면 리소스 목록을 검토하고 네임스페이스에 있는 리소스의 범위만 지정되는지 확인합니다. 또는 AMS 네임스페이스에 있는 리소스를 제외합니다. 이 결과는 정책이 지정된 서비스에 대한 태그 지정 권한을 부여하고 권한이 특정 태그 키/값으로 범위가 지정되지 않은 경우에 생성됩니다. 예를 들어 작업 수행을 요청할 때 태그 작업에 사용할 수 있는 키 또는 값의 범위를 좁히려면 <code>aws:RequestTag/tag key</code> 조건을 사용합니다. 따라서 이 문제를 해결하려면 이 조건 키를 사용하여 이름 공간의 키 또는 값을 제한합니다. 또는 AMS 네임스페이스의 값이 있는 Name 태그 키(<code>aws:RequestTag/Name</code>)를 거부합니다.
IAM 역할 신뢰 정책을 검증하는 동안 내부 오류가 발생했습니다.	이 결과는 CT 자동화에서 IAM Access Analyzer 서비스를 통해 IAM 역할 신뢰 정책에 대한 검증을 수행하는 동안 오류가 발생할 때 생성됩니다. 이 문제를 해결하려면 RFC를 다시 제출하십시오. 오류가 지속되면 AMS Operations에 문의하여 오류를 해결합니다.
고객 관리형 정책을 검증하는 동안 내부 오류가 발생했습니다.	이 결과는 CT 자동화에서 IAM Access Analyzer 서비스를 통해 고객 관리형 정책에 대해 타원형화를 수행하는 동안 오류가 발생할 때 생성됩니다. 이 문제를 해결하려면 RFC를 다시 제출하십시오. 오류가 지속되면 AMS Operations에 문의하여 오류를 해결합니다.

조사 결과	설명
액세스 분석기에서 찾을 수 없습니다 AWS ## . 역할 신뢰 정책에 대한 액세스 미리 보기 검사를 수행할 수 없습니다.	이 결과에서는 IAM Access Analyzer 리소스를 찾을 수 없을 때 생성됩니다 AWS 리전. AMS Operations에 문의하여 AWS 리전에서 IAM Access Analyzer 리소스 문제를 해결하고 생성합니다.
Role_Name 역할에 대한 잘못된 신뢰 정책	이 결과는 IAM 역할에 잘못된 신뢰 정책이 포함된 경우 생성됩니다. 문제를 해결하려면 신뢰 정책을 검토하여 유효한지 확인합니다.
IAM Access Analyzer에서 내부 오류가 발생했습니다. Role_Name 역할에 대한 액세스 미리 보기를 생성하지 못했습니다.	이 결과는 IAM Access Analyzer를 통해 역할에 대한 액세스 미리 보기를 생성하는 동안 자동화에서 오류가 발생할 때 생성됩니다. 이 문제를 해결하려면 RFC를 다시 제출하십시오. 오류가 지속되면 AMS Operations에 문의하여 오류를 해결합니다.
Role_Name 역할의 신뢰 정책에 대한 액세스 미리 보기를 생성하지 못했습니다.	이 결과는 IAM Access Analyzer를 통해 역할에 대한 액세스 미리 보기를 생성하는 동안 자동화에서 오류가 발생할 때 생성됩니다. 이 문제를 해결하려면 RFC를 다시 제출하십시오. 오류가 지속되면 AMS Operations에 문의하여 오류를 해결합니다.
나열된 SAML IdP를 검증하는 동안 내부 오류가 발생했습니다.	이 결과는 역할 신뢰 정책에 나열된 제공된 SAML IdPs를 검증하는 동안 자동화에 오류가 발생하면 생성됩니다. 이 문제를 해결하려면 RFC를 다시 제출하십시오. 오류가 지속되면 AMS Operations에 문의하여 오류를 해결합니다.
권한을 검증하는 동안 내부 오류가 발생했습니다 AWS Key Management Service.	이 결과는 제공된 정책에서 AWS KMS 키 권한을 검증하는 동안 자동화에 오류가 발생하면 생성됩니다. 이 문제를 해결하려면 RFC를 다시 제출하십시오. 오류가 지속되면 AMS Operations에 문의하여 오류를 해결합니다.

조사 결과	설명
나열된 관리형 정책 ARNs 검증하는 동안 내부 오류가 발생했습니다.	이 결과는 나열된 관리형 정책 ARNs을 검증하는 동안 자동화에 오류가 발생하면 생성됩니다. 이 문제를 해결하려면 RFC를 다시 제출하십시오. 오류가 지속되면 AMS Operations에 문의하여 오류를 해결합니다.
기본 <code>customer_deny_policy</code> 연결을 검증하는 동안 내부 오류가 발생했습니다.	이 결과는가 역할에 <code>customer_deny_policy</code> 연결되어 있는지 확인하는 동안 자동화에 오류가 발생하면 생성됩니다. 이 문제를 해결하려면 RFC를 다시 제출하십시오. 오류가 지속되면 AMS Operations에 문의하여 오류를 해결합니다.
<i>Role_Name</i> 역할에 대한 관리형 정책 ARN을 검증하는 내부 오류	이 결과는 역할에 대한 관리형 정책 ARNs을 검증하는 동안 자동화에 오류가 발생하면 생성됩니다. 이 문제를 해결하려면 RFC를 다시 제출하십시오. 오류가 지속되면 AMS Operations에 문의하여 오류를 해결합니다.
<i>Policy_name</i> 을 고객 정의 경계 정책에 대해 검증하는 내부 오류 <code>AWSManagedServicesIAMProvisionCustomerBoundaryPolicy</code>	이 결과는 사용자 지정 거부 목록을 포함하는 정책을 검증하는 동안 자동화에 오류가 발생하면 생성됩니다. 이 문제를 해결하려면 RFC를 다시 제출하십시오. 오류가 지속되면 AMS Operations에 문의하여 오류를 해결합니다.
고객 정의 경계 정책이 계정에 <code>AWSManagedServicesIAMProvisionCustomerBoundaryPolicy</code> 있습니다. 그러나 정책에는 권한을 부여하는 허용 문이 포함되어 있습니다. 정책에는 거부 문만 포함되어야 합니다.	이 결과는 사용자 지정 거부 목록이 포함된 정책에 권한을 부여하는 문이 포함된 경우 생성됩니다. 사용자 지정 거부 목록은 계정 내에 IAM 관리형 정책으로 존재하지만 권한 관리에 사용할 수 없습니다. 정책에는 AMS 자동 IAM 프로비저닝이 생성한 IAM 정책에서 해당 작업을 검증하고 거부하도록 하려는 거부 문만 포함되어야 합니다.

조사 결과	설명
문에는 조직에서 <i>Service_Name</i> 에 대해 정의한 권한이 있는 작업이 포함되어 있습니다. 거부문과 함께 이러한 작업을 제외하는 것이 좋습니다. 제한된 작업 목록을 참조하려면 계정에서 라는 정책을 참조하세요.	이 결과는 자동화가 사용자 지정 거부 목록에 정의한 정책에서 작업을 감지할 때 생성됩니다. 조사 결과를 해결하려면 정책 설명을 검토하고 사용자 지정 거부 목록에 정의된 작업을 제거하거나 해당 작업을 거부하는 거부 설명을 추가합니다.
역할에는 <i>POLICY_ARN</i> 이 연결되어 있어야 합니다. 관리형 정책 ARN 목록에 정책 ARNs 포함합니다.	생성 중인 역할에 <i>POLICY_ARN</i> 이 연결되어 있지 않은 경우 이 결과가 생성됩니다. 이 문제를 해결하려면 역할의 ManagedPolicyArns 필드에 <i>POLICY_ARN</i> 을 포함하고 다시 시도하세요.
<i>POLICY_ARN</i> 은 역할에서 분리할 수 없습니다. 관리형 정책 ARN 목록에 정책 ARNs 포함합니다.	이 결과는 업데이트 중에 <i>POLICY_ARN</i> 이 역할에서 분리된 경우 생성됩니다. 이 문제를 해결하려면 역할의 ManagedPolicyArns 필드에 <i>POLICY_ARN</i> 을 추가하고 다시 시도하세요.

AMS 자동 IAM 프로비저닝 권한 경계 확인

AMS 권한 경계 검사는 AMS에서 제공하는 기본 권한 경계 정책을 준수하는 데 도움이 됩니다. 이 정책은 AMS 자동 IAM 프로비저닝에서 거부한 작업 목록입니다. 이러한 제한된 작업이 포함된 프로비저닝 정책을 사용하려면 추가적인 명시적 위험 수락이 필요합니다. 여기에서 정책을 다운로드합니다. [boundary-policy.zip](#).

고객 정의 권한 경계 정책 검사를 사용하여 AMS 권한 경계 정책 기본값을 초과하는 거부 작업을 사용자 지정합니다. 관리 | 관리형 계정 | 읽기-쓰기 권한이 있는 AMS 자동 IAM 프로비저닝 | [활성화\(검토 필요\)](#)(ct-1706xvvk6j9hf) 변경 유형을 사용하여 AMS 자동 IAM 프로비저닝에 온보딩하는 경우 추가 제한 작업을 지정하는 사용자 지정 거부 작업 목록을 포함할 수 있습니다.

관리 | 관리형 계정 | 읽기-쓰기 권한이 있는 자동 IAM 프로비저닝 | [사용자 지정 거부 목록 업데이트](#)(ct-2r9xvd3sdsic0) 변경 유형을 사용하여 거부 작업 목록을 업데이트할 수 있습니다. 이 변경 유형을 실행AWSManagedServicesIAMProvisionAdminRole하려면 전용 IAM 역할을 사용해야 합니다.

Note

- 각 업데이트에 대한 포괄적인 거부 작업 목록을 제공해야 합니다. 이전 목록은 새 목록으로 대체됩니다.
- 거부 작업 목록에는 거부할 작업만 포함되어야 합니다. 허용 작업은 지원되지 않습니다.
- 거부 작업 목록은 계정 내에 라는 IAM 관리형 정책으로 상주합니다
다AWSManagedServicesIAMProvisionCustomerBoundaryPolicy. 정책은 어떤 역할
에도 연결되어서는 안 됩니다.
- AMS 자동 IAM 프로비저닝에서 거부된 작업을 나타내는 데 사용되는 권한 경계라는 용어는 IAM 권한 경계와 컨텍스트적 의미가 다릅니다. IAM 권한 경계는 정책이 런타임 시 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. IAM 권한 경계에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [정책 유형](#)을 참조하세요. AMS 자동 IAM 프로비저닝의 권한 경계를 사용하면 거부된 작업 목록과 같은 특정 권한 집합이 포함된 IAM 정책을 프로비저닝할 수 없습니다.

AMS 자동 IAM 프로비저닝 벤딩 및 오류 문제 해결

AMS 자동 IAM 프로비저닝을 사용할 때 문제가 발생할 수 있는 세 가지 방법이 있습니다.

- RFC 오류: 잘못된 입력과 같은 다양한 이유로 발생할 수 있습니다. 자세한 내용은 [AMS의 RFC 오류 문제 해결](#) 단원을 참조하십시오.
- SSM 오류: 잘못된 형식 지정과 같은 다양한 이유로 발생할 수 있습니다. 자세한 내용은 [Systems Manager Automation 문제 해결](#)을 참조하세요.
- 검증 검사 결과: 이는 자동 IAM 프로비저닝 실행에서 문제를 발견한 많은 검증 검사 중 하나에서 발생합니다. 검증 검사 목록과 수정할 권장 조치는 섹션을 참조하세요 [AMS에서 AMS 자동 IAM 프로비저닝에 대한 런타임 확인](#).

IAM 역할 및 프로파일을 사용하여 AMS에서 권한 설정

AMS는 AWS Identity and Access Management (IAM)를 사용하여 사용자, 액세스 키와 같은 보안 자격 증명, 사용자 및 애플리케이션이 액세스할 수 있는 리소스를 제어하는 AWS 권한을 관리합니다. AMS는 기본 IAM 사용자 역할과 기본 Amazon EC2 인스턴스 프로파일(기본 IAM 사용자 역할에 대한 리소스 액세스를 허용하는 문 포함)을 제공합니다.

새 IAM 사용자 역할 또는 인스턴스 프로파일 요청

AMS는 IAM 역할을 사용하여 페더레이션 서비스를 통해 사용자 권한을 설정하고 IAM 인스턴스 프로파일을 해당 IAM 역할의 컨테이너로 설정합니다.

배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 개체 또는 정책 생성(검토 필요) 변경 유형(ct-3dpd8mdd9jn1r)을 사용하여 사용자 지정 IAM 역할을 요청하거나 관리 | 애플리케이션 | IAM 인스턴스 프로파일 | 관리 생성 | 애플리케이션 | IAM 인스턴스 프로파일 | 생성(검토 필요) 변경 유형(ct-0ixp4ch2tiu04)을 사용하여 IAM 인스턴스 프로파일을 요청할 수 있습니다. 이 단원에서 각에 대한 설명을 참조하십시오.

Note

AMS에는 위험한 네임스페이스와 작업을 차단customer_deny_policy하는 IAM 정책이 있습니다. 이 정책은 기본적으로 모든 AMS 고객 역할에 연결되며 사용자에게는 거의 문제가 되지 않습니다. IAM 사용자 및 역할 요청에는이 정책이 포함되지 않지만 IAM 역할 요청에 customer_deny_policy를 자동으로 포함하면 AMS가 새 IAM 인스턴스 프로파일을 더 빠르게 배포할 수 있습니다. customer_deny_policy 정책의 제외를 요청할 수 있습니다. 그러나 이 요청은 가중치 기반 보안 검토를 거치며 보안상의 이유로 거부될 수 있습니다.

IAM 역할 정책 설명을 사용하여 권한 제한

AMS는 IAM 역할을 사용하여 페더레이션 서비스를 통해 사용자 권한을 설정합니다.

단일 계정 랜딩 존 AMS: [SALZ: 기본 IAM 사용자 역할을 참조하세요.](#)

다중 계정 랜딩 존 AMS: [MALZ: 기본 IAM 사용자 역할을 참조하세요.](#)

IAM 역할은 AWS 서비스 요청을 수행할 수 있는 권한 집합을 정의하는 IAM 엔터티입니다. IAM 역할은 특정 사용자 또는 그룹과 연결되지 않습니다. 대신 신뢰할 수 있는 엔터티는 IAM 사용자, 애플리케이션 또는 Amazon EC2와 같은 AWS 서비스와 같은 역할을 수임합니다. 자세한 내용은 [IAM 역할](#)을 참조하십시오.

Policy 요청 필드 아래에 보다 제한적인 IAM 정책을 전달하여 AWS 보안 토큰 서비스(STS) API 작업 [AssumeRole](#)을 사용하여 AMS IAM 사용자 역할을 수임하는 사용자에게 대해 원하는 정책의 범위를 좁힐 수 있습니다.

CT 액세스를 제한하는 데 사용할 수 있는 정책 설명의 예가 다음에 제공됩니다.

구성된 Active Directory(AD) 그룹과 AWS Security Token Service(STS) API 작업 [AssumeRole](#)을 사용하여 특정 변경 유형(CTs. 아래 표시된 정책 설명을 사용하여 다양한 방법으로 CT 액세스를 제한할 수 있습니다.

모든 AMS API 호출(amscm 및 amsskms) 및 모든 변경 유형에 대한 액세스를 허용하는 기본 IAM 인스턴스 프로파일의 AMS 변경 유형 문:

```
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
    "*"
  ]
}
```

1. 지정된 두 CT에 대해서만 액세스 및 모든 작업을 허용하는 문CTs 여기서 "Action"은 AMS API 작업(amscm 또는 amsskms)이고 "Resource"는 기존 변경 유형 IDs 및 버전 번호를 나타냅니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "amscm:*",
      "Resource": [
        "arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
        "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"
      ]
    }
  ]
}
```

2. 지정된 두 CT에서만 CreateRfc, UpdateRfc 및 SubmitRfc에 대한 액세스를 허용하는 문CTs
3. 사용 가능한 모든 CT에서 CreateRfc, UpdateRfc 및 SubmitRfc에 대한 액세스를 허용하는 문: CTs

4. 제한된 CT의 모든 작업에 대한 액세스를 거부하고 다른 CTs

Amazon EC2 IAM 인스턴스 프로파일로 권한 제한

IAM 인스턴스 프로파일은 인스턴스가 시작될 때 Amazon EC2 인스턴스에 역할 정보를 전달하는 데 사용할 수 있는 IAM 역할의 컨테이너입니다.

현재 인스턴스에 로그인customer-mc-ec2-instance-profile하는 사용자가 아닌 인스턴스에서 실행 중인 애플리케이션에 권한을 부여하는 AWS Managed Services(AMS) 기본 인스턴스 프로파일이 하나 있습니다. 다른 인스턴스에도 액세스 권한을 부여하지 않고 인스턴스에 액세스 권한을 부여하려는 경우 기본 인스턴스 프로파일을 수정하거나 새 인스턴스 프로파일을 생성할 수 있습니다. 관리 | 애플리케이션 | IAM 인스턴스 프로파일 | 변경 유형 생성(ct-0ixp4ch2tiu04)을 사용하여 새 IAM 인스턴스 프로파일을 요청할 수 있습니다. RFC를 제출할 때 자체 인스턴스 프로파일을 구성하고 이를 InstanceProfileDescription으로 포함하거나 원하는 변경 사항을 AMS(동일한 필드 사용)에 알릴 수 있습니다. 수동 CT이므로 AMS는 변경 사항을 승인해야 하며 이에 대해 연락을 드릴 것입니다.

Amazon IAM 정책에 익숙하지 않은 경우 중요 정보는 [IAM 정책 개요](#)를 참조하세요. 좋은 블로그 게시물인 [Amazon EC2 리소스 수준 권한 설명도 있습니다](#). AMS는 현재 리소스 기반 액세스 제어를 지원하지 않지만 IAM 역할 정책을 사용하여 리소스 수준 제어를 지원합니다(차이에 대한 설명은 [AWS IAM으로 작업하는 서비스](#)를 참조하세요).

단일 계정 랜딩 존 AMS:

기본 AMS IAM 인스턴스 프로파일이 부여하는 권한 표를 보려면 [EC2 IAM 인스턴스 프로파일](#)로 이동합니다.

AD FS 클레임 규칙 및 SAML 설정

AWS Managed Services(AMS)에 대한 ActiveDirectory Federation Services(AD FS) 클레임 규칙 및 SAML 설정 AWS Managed Services

AD FS를 설치하고 구성하는 방법에 대한 step-by-step 지침은 [Windows Active Directory, ADFS 및 SAML 2.0을 사용하여 AWS에 페더레이션 활성화](#)를 참조하세요.

ADFS 클레임 규칙 구성

ADFS 구현이 이미 있는 경우 다음을 구성합니다.

- 신뢰 당사자 신뢰

• 클레임 규칙

신뢰 당사자 신뢰 및 클레임 규칙 단계는 [Windows Active Directory, AD FS 및 SAML 2.0 블로그를 사용하여 AWS에 페더레이션 활성화](#)에서 수행됩니다.

• 클레임 규칙:

- Nameid: 블로그 게시물당 구성
- RoleSessionName: 다음과 같이 구성
 - 클레임 규칙 이름: **RoleSessionName**
 - 속성 저장소: **Active Directory**
 - LDAP 속성: **SAM-Account-Name**
 - 발신 클레임 유형: **https://aws.amazon.com/SAML/Attributes/RoleSessionName**
 - AD 그룹 가져오기: [블로그 게시물당 구성](#)
 - 역할 클레임: 다음과 같이 구성

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^\d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =  
  RegExReplace(c.Value, "AWS-([^\d]{12})-", "arn:aws:iam:$1:saml-provider/  
  customer-readonly-saml,arn:aws:iam:$1:role/"));
```

웹 콘솔

아래 링크를 사용하여 **[ADFS-FQDN]**을 ADFS 구현의 FQDN으로 대체하여 AWS 웹 콘솔에 액세스할 수 있습니다.

[https://\[ADFS-FQDN\]/adfs/ls/IdpInitiatedSignOn.aspx](https://[ADFS-FQDN]/adfs/ls/IdpInitiatedSignOn.aspx)

IT 부서가 그룹 정책을 통해 사용자 집단에 위 링크를 배포할 수 있습니다.

SAML을 사용한 API 및 CLI 액세스

SAML을 사용하여 API 및 CLI 액세스를 구성하는 방법.

Python 패키지는 아래 블로그 게시물에서 제공됩니다.

- NTLM: [SAML 2.0 및 AD FS를 사용하여 페더레이션 API 및 CLI 액세스를 구현하는 방법](#)
- 양식: [SAML 2.0을 사용하여 페더레이션 API/CLI 액세스를 위한 일반 솔루션을 구현하는 방법](#)
- PowerShell: [Windows PowerShell을 사용하여 AWS에 대한 페더레이션 API 액세스를 설정하는 방법](#)

스크립트 구성

1. Notepad++를 사용하여 기본 리전을 올바른 리전으로 변경합니다.
2. Notepad++를 사용하여 테스트 및 개발 환경에 대한 SSL 확인 비활성화
3. Notepad++를 사용하여 idpentryurl 구성

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?  
loginToRp=urn:amazon:webservices
```

Windows 구성

아래 지침은 python 패키지에 대한 것입니다. 생성된 자격 증명은 1시간 동안 유효합니다.

1. [python\(2.7.11\) 다운로드 및 설치](#)
2. [AWS CLI 도구 다운로드 및 설치](#)
3. AMS CLI를 설치합니다.
 - a. 클라우드 서비스 제공 관리자(CSDM)가 제공한 AMS 배포 가능 zip 파일을 다운로드하고 압축을 풉니다.

여러 디렉터리와 파일을 사용할 수 있습니다.

- b. 운영 체제에 따라 관리형 클라우드 배포 가능 -> CLI -> Windows 또는 관리형 클라우드 배포 가능 -> CLI -> Linux/macOS 디렉터리를 엽니다.

Windows의 경우 적절한 설치 관리자를 실행합니다(이 방법은 Windows 32 또는 64비트 시스템에서만 작동함).

- 32비트: ManagedCloudAPI_x86.msi
- 64비트: ManagedCloudAPI_x64.msi

Mac/Linux의 경우 MC_CLI.sh라는 파일을 실행합니다. 명령을 실행하여이 작업을 수행할 수 있습니다sh MC_CLI.sh. amscm 및 amsskms 디렉터리와 그 내용은 MC_CLI.sh 파일과 동일한 디렉터리에 있어야 합니다.

- c. 기업 자격 증명을 AWS와의 페더레이션(AMS 기본 구성)을 통해 사용하는 경우 페더레이션 서비스에 액세스할 수 있는 자격 증명 관리 도구를 설치해야 합니다. 예를 들어이 AWS 보안 블로그 [SAML 2.0 및 AD FS를 사용하여 연합 API 및 CLI 액세스를 구현하는 방법을](#) 사용하여 자격 증명 관리 도구를 구성할 수 있습니다.
- d. 설치 후 aws amscm help 및 aws amsskms help하여 명령과 옵션을 확인합니다.

4. 필요한 SAML 스크립트 다운로드

c:\aws\scripts로 다운로드

5. [PIP 다운로드](#)

c:\aws\downloads로 다운로드

6. PowerShell을 사용하여 PIP 설치

```
<pythondir>.\python.exe c:\aws\downloads\get-pip.py
```

7. PowerShell을 사용하여 boto 모듈 설치

```
<pythondir\scripts>pip 설치 boto
```

8. PowerShell을 사용하여 요청 모듈 설치

```
<pythondir\scripts>pip 설치 요청
```

9. PowerShell을 사용하여 요청 보안 모듈 설치

```
<pythondir\scripts>pip 설치 요청[보안]
```

10. PowerShell을 사용하여 beautifulsoup 모듈 설치

```
<pythondir\scripts>pip 설치 beautifulsoup4
```

11. PowerShell을 사용하여 사용자 프로파일에 .aws라는 폴더를 생성합니다(%userprofile%\aws).

```
mkdir .aws
```

12. PowerShell을 사용하여 .aws 폴더에 자격 증명 파일 생성

```
New-Item 자격 증명 -유형 파일 -force
```

자격 증명 파일에 파일 확장자가 없어야 합니다.

파일 이름은 모두 소문자여야 하며 이름 자격 증명이 있어야 합니다.

13. 메모장으로 자격 증명 파일을 열고 올바른 리전을 지정하여 다음 데이터를 붙여 넣습니다.

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. PowerShell, SAML 스크립트 및 로그인 사용

<pythondir>.\python.exe c:\aws\scripts\samlapi.py

사용자 이름: [USERNAME]@upn

수입할 역할을 선택합니다.

Linux 구성

생성된 자격 증명은 1시간 동안 유효합니다.

1. WinSCP를 사용하여 SAML 스크립트 전송
2. WinSCP를 사용하여 루트 CA 인증서 전송(테스트 및 개발 무시)
3. 신뢰할 수 있는 루트 인증서에 ROOT CA 추가(테스트 및 개발 무시)

\$ openssl x509 -in [certname].cer -out certificate.pem에 대한 정보 제공(테스트 및 개발 무시)

/etc/ssl/certs/ca-bundle.crt 파일의 끝에 certificate.pem의 콘텐츠 추가((테스트 개발의 경우 무시)

4. home/ec2-user 5에서 .aws 폴더 생성

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```


5. WinSCP를 사용하여 자격 증명 파일을 .aws 폴더로 전송합니다.

6. Boto 모듈 설치

```
$ sudo pip install boto
```

7. 요청 모듈 설치

```
$ sudo pip 설치 요청
```

8. beautifulsoup 모듈 설치

```
$ sudo pip install beautifulsoup4
```

9. 스크립트를 home/ec2-user에 복사

필요한 권한 설정

스크립트 실행: samlapi.py

네트워크 ACL로 제한

네트워크 액세스 제어 목록(NACL)은 하나 이상의 서브넷으로 들어오고 나가는 트래픽을 제어하는 방화벽 역할을 하는 VPC의 선택적 보안 계층입니다. 보안 그룹과 비슷한 규칙으로 네트워크 ACL을 설정하여 VPC에 보안 계층을 더 추가할 수 있습니다. 보안 그룹과 네트워크 ACLs의 차이점에 대한 자세한 내용은 [보안 그룹과 네트워크 ACLs](#).

그러나 AMS 관리형 다중 계정 랜딩 존에서 AMS가 인프라를 효과적으로 관리하고 모니터링하기 위해 NACLs 사용은 다음 범위로 제한됩니다.

- 다중 계정 랜딩 존 코어 계정, 즉 관리 계정, 네트워킹, 공유 서비스, 로깅 및 보안에서는 NACLs이 지원되지 않습니다.
- NACLs은 "거부" 목록으로만 사용되고 AMS 모니터링 및 관리 작업을 허용하는 "모두 허용"이 있는 경우 다중 계정 랜딩 존 애플리케이션 계정에서 지원됩니다.

대규모 다중 계정 환경에서는 중앙 집중식 송신 방화벽과 같은 기능을 활용하여 AMS 다중 계정 랜딩 존의 아웃바운드 트래픽 및/또는 AWS 전송 게이트웨이 라우팅 테이블을 제어하여 VPCs.

Outposts의 AMS

[AWS Outposts](#)는 AMS 관리형 랜딩 존을 고객 데이터 센터로 확장하는 관리형 하드웨어 솔루션입니다. 에 대한 AMS 지원을 통해 AMS에서 제공하는 클라우드 전문 지식, 비용 절감 및 표준화된 플랫폼을 찾는 AWS Outposts고객은 더 이상 내부 리소스 호스팅으로 제한되지 않습니다 AWS 리전. AMS를 켜면 온프레미스 요구 사항이 있는 AWS Outposts고객이 이제 AMS에서 제공하는 패치 AWS적용, 백업, 프로비저닝, 인스턴트 관리, 비즈니스 연속성 및 비용 최적화 서비스를 활용하면서 현대화할 수 있습니다.

AMS 다중 계정 랜딩 존 또는 단일 계정 랜딩 존 계정에서 AWS Outposts 이 활성화되면 기존 AMS 변경 관리 프로세스에 따라 AWS 리소스를 프로비저닝하고 관리할 수 있습니다. AMS 호스팅 인프라는 AWS Outposts특정 서브넷을 지정하여 관리할 수 있습니다. AWS Outposts 수명 주기는 AWS Outposts 자체 프로비저닝 서비스 역할을 사용하여 AWS Outposts 콘솔에서 직접 관리할 수 있습니다.

역할에 대한 자세한 내용은 섹션을 참조하세요 [AWS Outposts](#).

AWS Outposts 설치 및 운영 관리

AWS Outposts 진행 중인 AMS에 대한 온보딩은 다음으로 구성됩니다.

1. Outposts 계획
2. 주문 검증
3. AMS에 Outpost 온보딩
4. 수명 주기 관리

AWS Outposts 계획

AWS Outposts 계획 중에 AWS Outposts 사용 사례에 대한 AMS를 식별하고 AMS 계정 팀 및 AWS Outposts 담당자를 포함한 주요 이해관계자를 참여시켜 용량 전략을 조정합니다.

1. 에서 AMS AWS Outposts 가 필요한 사용 사례가 식별되면 AMS 계정 팀을 참여시켜 용량 계획에 대해 논의합니다.
2. AWS Outposts 용량 요구 사항이 결정되면 AMS 계정 팀이 AWS Outposts 서비스 팀을 참여시켜 AWS Outposts 온보딩 계획, 역할 및 책임을 논의합니다. 이 시간 동안 AWS Outposts 단일 연락 지점(SPOC)이 할당됩니다. AWS Outposts SPOC는 AWS Outposts 크기 조정 요구 사항을 완료하는데 도움이 됩니다.

AWS Outposts 주문 검증

주문 확인 중에 AWS Outposts 사이트를 생성하고 AWS Outposts 콘솔에서 직접 또는 AWS Outposts 계정 담당자를 통해 필요한 용량을 주문합니다.

AMS 계정 팀인 AWS Outposts 팀이 조정되면 변경 유형 ID ct-3qe6io8t6jtny를 사용하여 자체 프로비저닝된 서비스 역할을 요청 AWS Outposts 하여 사이트를 AWS Outposts 생성하고 AWS Outposts 콘솔에서 직접 주문할 수 있습니다.

또는 AWS Outposts SPOC를 통해 Outpost 사이트 및 주문을 생성할 수 있습니다. AWS Outposts SPOC는 사이트 및 주문 검증, AWS Outposts 설치 중에 사용자와 AMS 계정 팀에 상태 업데이트를 계속 제공합니다.

AWS Outposts AMS에 온보딩

AMS 관리형 VPC에서 AWS Outposts 유닛이 활성화되면 Outposts 하드웨어의 가용성, 용량, 예외 및 네트워크 연결을 추적하기 위해에 모니터를 생성하도록 요청할 수 있습니다. 다음에 설명된 모니터링 배포 단계에 따라 AMS에서 AWS Outposts 하드웨어를 적극적으로 모니터링합니다.

1. AWS Outposts 가 설치되고 활성화되면 관리 | 기타 | 기타 | 생성(ct-1e1xtak34nx76) 변경 유형을 사용하여 RFC와 함께 다음 템플릿을 제출하여 AWS Outposts특정 모니터링을 요청할 수 있습니다. AMS 작업은 AWS Outposts 서브넷이 AMS 내부 도구에서 추적되도록 합니다.

- AWS Outposts ID
- 서브넷 CIDR
- 권장 AWS Outposts 경보:
 - InstanceFamilyCapacityAvailabilityAlert
 - InstanceTypeCapacityAvailabilityAlert
 - EBSVolumeTypeCapacityAvailabilityAlert
 - CapacityExceptionsAlert
 - Direct Connect ConnectionAlert
- 위의 각 알림에 대해 다음 파라미터를 지정합니다.
 - 통계("평균"이 권장됩니다. 기타 옵션에는 합계, 최대값, 최소값, 샘플 수 및 p90)이 포함됩니다.
 - 기간("5분"이 권장됩니다. 다른 옵션으로는 10초 및 30초, 1분, 5분 및 15분, 1시간 및 6시간, 1일)이 있습니다.
 - 임계값 유형("정적"이 권장됩니다. "이상"도 옵션입니다.)
 - 조건("호출 수가 보다 클 때마다", "같음", "작음"도 옵션입니다.)

- 조건 값("25%"은 기본적으로 구성됩니다. 다른 양의 정수도 허용됩니다.)
- 알림 주제(AMS 작업 주제가 자동으로 할당됩니다. 그러나 다른 주제 또는 사용자 지정 주제도 추가할 수 있습니다.)

2. 모니터링 및 운영 지원

- AMS 작업은 네트워크 연결 해제 또는 구성 요소 장애에 대한 AWS Outposts 지표를 모니터링 합니다. AMS 작업은 AWS Outposts 문제에 대한 첫 번째 대응 서비스를 제공하고 필요한 경우 Premium 지원 또는 EC2 지원으로 에스컬레이션합니다.
- AMS 작업을 사용하여 AWS Outposts 단위와 관련된 문제를 해결할 수 있습니다.

3. EC2 인스턴스 상태 또는 시스템 상태 확인에 실패하면 AMS 작업은 기존 프로세스를 따라 인스턴스를 다시 온라인 상태로 전환합니다. 재시작에 실패하거나 AWS Outposts 용량이 충분하지 않은 경우 AMS 운영 팀원이 사용자에게 직접 알려 다음 단계를 결정합니다.

AWS Outposts 수명 주기 관리

AWS Outposts 가 AMS 계정에 온보딩되면 가용성, 용량 또는 네트워크 예외가 발생할 경우 알림을 받게 됩니다. 콘솔 또는 AWS Outposts SPOC를 AWS Outposts 통해 AWS Outposts 직접 폐기할 수 있습니다.

AWS Outposts 셀프 서비스 프로비저닝 서비스 역할 또는 개발자 모드를 사용하여 AWS Outposts 콘솔에서 AWS Outposts 직접을 관리할 수 있습니다. CSDM 또는 AWS Outposts 단일 연락 지점(SPOC)을 AWS Outposts 통해를 요청할 수도 있습니다.

둘 이상의 배포하여에서 고가용성을 달성할 AWS Outposts 수 있습니다 AWS Outposts. 둘 이상을 구성하면 Amazon Relational Database Service 인스턴스에 대한 다중 가용 영역 옵션이 AWS Outposts 활성화됩니다.

에서 AMS 관리형 리소스 프로비저닝 AWS Outposts

AMS 계정 AWS Outposts (단일 계정 랜딩 존, 다중 계정 랜딩 존 및 Accelerate 계정)의 (예: Amazon EC2, Amazon EMR, Amazon EKS, Amazon ECS, Amazon EBS 및 Amazon S3)에서 AWS 호스팅되는 리소스 프로비저닝에는의 리소스와 동일한 AMS 지원 수준이 적용됩니다 AWS 리전. AMS 변경 관리, 셀프 서비스 프로비저닝 서비스 또는 개발자 모드를 사용하여에서 생성된 리소스를 생성하고 수정할 수 있습니다 AWS Outposts.

현재 모든 인스턴스 유형(M5/M5d, C5/C5d, R5/R5d, I3en, G4dn), Amazon Elastic Block Store, Amazon Elastic Container Service, Amazon Elastic Kubernetes Service, Amazon EMR, Amazon Relational Database Service DBs, Application Load Balancer 및 App Mesh Envoy 프록시를에서 직접

사용할 수 있습니다 AWS Outposts. 이러한 리소스는 기존 리전의 리소스와 동일한 AMS 작업 지원을 받을 수 있습니다.

의 AMS 제한 사항 AWS Outposts

- AWS Outposts호스팅 리소스에 대한 운영 지원은 일관된 네트워크 연결에 따라 달라집니다. AWS Outposts 네트워크 연결 해제는 AMS 작업이 연결 해제된 AWS Outposts 장치에서 발생하는 인시던트 또는 문제를 해결할 수 없도록 합니다. 서비스 수준 비상 상황에 대한 AWS Outposts AMS는 업데이트된 [AWS 서비스 수준 계약\(SLAs\)을 참조하세요](#).
- Amazon Relational Database Service:
 - RDS 변경 유형 생성(ct-2z60dyvto9g6c)은 기본적으로 다중 AZ를 활성화하고 DB 서브넷 그룹이 필요합니다. DB 서브넷 그룹에는 별도의 가용 영역(AZ) 2개에 서브넷 2개가 필요합니다. 하나만 있는 경우는 단일 AZ AWS Outposts 에만 할당되므로 DB 서브넷 그룹을 AWS Outposts생성하는 것은 문제입니다. 이 제한을 피하려면 다음 지침을 따르세요.
 1. 관리 | 기타 | 기타 CT가 있는 RFC를 통해 DB 서브넷 그룹을 요청하고에서 서브넷을 지정합니다 AWS Outposts.
 2. RDS를 배포할 사용자 지정 CFN 템플릿을 생성하고 이전 단계에서 생성된 서브넷 그룹을 AWS Outposts지정합니다. 이에 대한 자세한 내용은 [사용자 지정 리소스](#)를 참조하세요.
 3. AMS가 AMS CFN 수집 CT(ct-36cn2avfrrj9v)를 통해 대상 RDS 인스턴스가 포함된 CFN 템플릿을 배포하도록 요청합니다.
 4. 현재 RDS for AWS Outposts 는 RDS Service의 제한으로 인해 지표와 로그를 제공하지 않습니다.
 - 워크로드 수집(WIGs): Linux WIGs 사전 WIGsEC2 인스턴스가AWS Outposts 서브넷이 아닌 경우에만 작동합니다. 그 이유는 Linux WIGs 기본적으로 m4.large를 사용하여 첫 번째 EC2 인스턴스의 서브넷에 WIGs 노드를 생성하기 때문입니다. AWS Outposts 에는 해당 인스턴스 유형이 없으므로 WIGs는 작업자 노드를 시작할 수 없습니다. 이에 대한 해결 방법은AWS Outposts 서브넷이 아닌에서 초기 EC2 인스턴스를 생성한 다음 대상 인스턴스를 생성할 수 있는 것입니다 AWS Outposts. 또한 현재는 C5, C5d, M5, M5d, R5, R5d, G4 및 I3en을 포함한 Nitro 기반 EC2 인스턴스 유형만 지원됩니다 AWS Outposts.
 - Amazon Elastic Block Store(EBS): AWS Outposts Amazon 리소스 번호(ARN)를 CT에 대한 입력 파라미터로 제공하지 않으므로 볼륨이 AWS 대신에서 생성 AWS Outposts 되므로 EBS 볼륨 CT(ct-16xg8qguovg2w) 생성이 작동하지 않습니다.
 - 네트워크 연결: 네트워크 연결은 AWS Outposts 팀당 사용자의 책임입니다.
 - AWS Outposts 결제 및 엔터프라이즈 지원 요구 사항의 특성으로 인해 비 AMS 계정에서 AWS Outposts 활성화된 브라운필드 및 계정 탈취:는 AMS로 전환할 수 없습니다.

AWS Outposts 규정 준수에 대한 AMS

AWS Outposts 규정 준수 증명에 대한 AMS

AWS Outposts 컨트롤 플레인인 HIPAA 적격, PCI 및 ISO 규정 준수를 증명했습니다. 그러나 AWS Outposts 컨트롤 플레인의 AMS는 증명되지 않았습니다 AWS Outposts. 이러한 이유로 고객은 환경에서 규정 준수 증명 AMS를 AWS Outposts 사용하는 것이 좋습니다.

Outpost 유닛에서 리소스 생성을 제어하려면 표준 AMS 관리형 계정에서 과도한 개발자 액세스를 방지하기 위해 Outpost에 대한 개발자 액세스를 분리하는 것이 좋습니다.

FedRAMP 규정 준수가 필요한 AMS 관리형 워크로드

무엇보다도 컨트롤 플레인 데이터가에서 AMS 관리 계정으로 흐르므로 AMS 관리 계정의 규정 준수 AWS Outposts 여부를 먼저 평가해야 합니다.

FedRAMP 인증이 필요하고 AMS 계정 구조가 규정을 준수하는 경우 이미 필요한 인증을 보유하고 모든 서비스 링크 어플라이언스를 소유한(또는 이미 송신 데이터를 암호화하는) 데이터 센터 공급 업체를 활용하는 것이 좋습니다.

마지막으로 계정 팀과 협력하여 데이터를 로 제한 AWS Outposts 하고 Outpost를 호스팅하는 계정에 리전 내 리소스가 생성되지 않도록 하는 SCP를 배포하여 추가 데이터 보호를 적용할 수 있습니다.

AMS 계정의 기존 규정 준수에 미치는 영향

를 사용하는 계정은 규제 데이터가 사용되지 AWS Outposts 않고 계정이 논리적으로 분리되어 있는 한 규정 준수를 위해 재테스트할 필요가 없습니다. AMS 관리 계정은 교차 계정 인증/권한 부여 및 수신/송신 데이터 흐름이 VPCs. 따라서 규정 미준수 Outpost 계정과 기존 규정 준수 애플리케이션 계정이 모두 동일한 조직(공유 서비스, 네트워킹, 로깅, 마스터, 보안 AMS 서비스 포함)에 있더라도 데이터가 논리적으로 분리되므로 규정 준수 애플리케이션 계정은 여전히 규정 준수를 유지합니다.

AMS AWS Outposts FAQs

에서 AMS 지원을 받을 수 있는 사용 사례는 무엇입니까 AWS Outposts?

의 AMS는 짧은 지연 시간(예: 공장 로봇 관리 및 메인프레임 마이그레이션), 엣지 컴퓨팅(예: 원격 워크스테이션 및 엣지 데이터 스트리밍) 및 대규모 데이터 전송 부하가 필요한 워크로드를 갖춘 검증된 클라우드 운영 모델이 필요한 기업에서 활용할 AWS Outposts 수 있습니다.

왜 이 기능을 사용해야 하나요?

AMS는 AWS Outposts 하드웨어에 대한 모니터링과 모든 AWS Outposts 하드웨어 문제에 대한 첫 번째 응답을 제공합니다. 또한 다음에서 호스팅되는 모든 관리형 리소스에 대한 기능을 지원합니다. AWS Outposts

- 로깅, 모니터링, 가드레일 및 이벤트 관리
- 연속성 관리
- 보안 및 액세스 관리
- 패치 관리
- 변경 관리
- 자동 및 셀프 서비스 프로비저닝 관리
- 인시던트 및 문제 관리
- 보고(하 AWS Outposts 드웨어에 대한 보고는 처음에의 AMS에서 지원되지 않음 AWS Outposts)
- 서비스 요청 관리
- 개발자 모드
- 엔터프라이즈 지원

이 기능은 어떻게 사용하나요?

AWS Outposts 계획: AWS Outposts 계획 중에 AWS Outposts 사용 사례에 대한 AMS를 식별했으며 AMS 계정 팀 및 AWS Outposts 담당자를 포함한 주요 이해관계자를 참여시켜 용량 전략을 조정합니다.

주문 검증: 주문 검증 중에 AWS Outposts 사이트를 생성하고 AWS Outposts 콘솔에서 직접 또는 AWS Outposts 계정 담당자를 통해 필요한 용량을 주문합니다.

AWS Outposts AMS에 온보딩: AMS 관리형 VPC에서 AWS Outposts 유닛이 활성화되면 AMS 사용 설명서()의 템플릿을 사용하여 변경 요청(RFC)을 제출하여 AMS 계정에 AWS Outposts 온보딩하도록 요청할 수 있습니다 [AWS Outposts](#). 그런 다음 AMS 작업은 서브넷을 생성하고 RFC에 제공된 입력을 사용하여 Outpost를 모니터링합니다.

수명 주기 관리: AWS Outposts 가 AMS 계정에 온보딩되면 가용성, 용량 또는 네트워크 예외에 대한 알림을 받습니다. AWS Outposts 콘솔 또는 AWS Outposts 단일 연락처(SPOC)를 통해 직접 폐기 AWS Outposts 할 수 있습니다.

AMS의 제한 사항은 무엇입니까 AWS Outposts?

데이터 레지던시(예: 국가별 데이터 현지화 법률 등) 사용 사례는 아직 AMS에 대해 검증되지 않았습니다 AWS Outposts.

AWS Outposts 비 AMS 계정에서 활성화되는 AWS Outposts 결제 및 엔터프라이즈 지원 요구 사항의 특성으로 인해 AMS로 전환할 수 없습니다.

AWS Outposts 컨트롤 플레인인 HIPAA 적격, PCI 및 ISO 규정 준수를 증명했습니다. 그러나 AWS Outposts 컨트롤 플레인의 AMS는 증명되지 않았습니다 AWS Outposts. 이러한 이유로 고객은 환경에서 규정 준수 증명 AMS를 AWS Outposts 사용하는 것이 좋습니다.

이 기능을 옵트아웃할 수 있나요?

AMS 환경 AWS Outposts 으로의 프로비저닝은 선택 사항입니다. AMS 계정에 배포된 후에는 더 이상 필요하지 않은 경우 언제든지 AWS Outposts 콘솔을 통해 프로비저닝을 해제할 AWS Outposts 수 있습니다.

의 AMS는 어떻게 청구 AWS Outposts 되나요?

AWS Outposts 요금에 대한 AMS 상승은 그룹 B 티어에 적용됩니다.

AMS 서비스 수준 계약은에 맞게 어떻게 변경되나요 AWS Outposts?

인시던트 관리는 AWS Outposts 가용성에 따라 달라집니다. AWS Outposts 가용성은 고객의 책임인 고객 네트워크 가용성에 따라 달라집니다. AWS Outposts 가용성은 AWS Outposts 서비스 수준 계약에 따라 달라지는 AWS Outposts 하드웨어 가동 시간도 따릅니다.

FAQ도 [AWS Outposts FAQs](#).

AMS에서 태그 사용

주제

- [AMS 인프라 자동 태그 지정](#)
- [AMS 권장 태그](#)
- [대량 업데이트 정보 태그 지정](#)

태그를 제공하는 것은 큰 가치가 있을 수 있습니다. 자세한 내용은 [Amazon EC2 리소스 태그 지정](#)을 참조하세요.

Amazon S3 버킷 또는 AWS Elastic Load Balancer(ELB)와 같은 인스턴스를 생성하는 RFCs는 일반적으로 최대 7개의 태그(키/값 페어)를 추가할 수 있는 스키마를 제공합니다. Management | Advanced stack components | Amazon S3S3 storage | Update CT를 제출하여 S3 버킷에 태그를 더 추가할 수 있

습니다. Amazon EC2, Amazon EFS, Amazon RDS 및 다중 계층(HA 2계층 및 HA 1계층) 스키마는 최대 50개의 태그를 허용합니다. 태그는 스키마의 ExecutionParameters 부분에 지정됩니다.

AMS 콘솔을 사용하는 경우 태그를 추가하려면 추가 구성 보기를 활성화해야 합니다.

Tip

많은 CT 스키마에는 스키마 상단에 Description 및 Name 필드가 있습니다. 이러한 필드는 스택 또는 스택 구성 요소의 이름을 지정하는 데 사용되며 생성 중인 리소스의 이름은 지정되지 않습니다. 일부 스키마는 생성 중인 리소스의 이름을 지정하는 파라미터를 제공하며 일부는 그렇지 않습니다. 예를 들어 Amazon EC2 스택 생성을 위한 CT 스키마는 Amazon EC2 인스턴스의 이름을 지정하는 파라미터를 제공하지 않습니다. 이렇게 하려면 "Name" 키와 이름을 지정할 값을 사용하여 태그를 생성해야 합니다. 이러한 태그를 생성하지 않으면 Amazon EC2 인스턴스가 이름 속성 없이 Amazon EC2 콘솔에 표시됩니다.

태그 제한이 있나요? 예:

- 태그는 대/소문자를 구분합니다.
- 최대 키 길이는 유니코드 문자 128자입니다.
- 최대 값 길이는 유니코드 문자 256자입니다.
- 리소스당 최대 태그 수는 50개입니다.
- aws:는 예약된 접두사입니다.
- AWS생성 태그의 이름과 값에는 사용자가 할당할 수 없는 aws: 접두사가 자동 할당됩니다. 비용 할당 보고서에는 사용자가 정의한 태그 이름에 접두사 user:가 포함됩니다.
- 각 리소스에 대해 각 키는 한 번만 사용해야 합니다. 동일한 리소스에서 동일한 키를 두 번 사용하려고 하면 요청이 거부됩니다.
- 허용되는 문자는 유니코드 문자, 공백, 숫자 및 특수 문자 + - = . _ : /입니다.

태그를 지원하는 AWS 리소스 유형은 무엇입니까? [리소스당 최대 50개의 태그를 AWS 사용하여 리소스 구성을 참조하세요.](#)

AMS 인프라 자동 태그 지정

AMS는 배포 | 고급 스택 구성 요소 | 태그 | 생성(검토 필요) 변경 유형(ct-0176f0n99vcps)을 사용하여 변경 요청(RFC)을 통해 다중 계정 랜딩 존(MALZ) 및 단일 계정 랜딩 존(SALZ) 계정에서 관리 목적으로

로 AMS가 생성한 모든 리소스에 태그를 지정할 수 있습니다. 이렇게 하면 관리 목적으로 AMS에서 생성한 리소스를 식별하는 데 도움이 될 수 있습니다.

AMS는 이름 지정 표준에 따라 AMS 생성 리소스를 자동으로 식별하고 리소스에 "AppName", "AppId", "AMSResource", "EnvironmentType" 등의 태그 키와 값이 있는지 확인할 수 있습니다. 태그 키가 없거나 값이 비어 있는 경우 해당 태그-키는 태그-값이 "AMSInfrastructure"인 AMS에서 자동으로 생성할 수 있습니다.

조직의 태그 지정 표준에 따라 AMS 생성 리소스에서 원하는 태그를 사용자 지정할 수 있습니다. AMS에 요청을 제출할 때 자체 태그 키와 태그 값을 포함할 수 있습니다. AWS 태그 이름 지정 표준: [태그 지정 모범 사례](#) 준수

Note

MALZ 계정의 경우 AMS 인프라의 사용자 지정 태그 지정은 애플리케이션 계정에서만 지원됩니다. 코어 계정의 사용자 지정 태그 지정은 현재 지원되지 않습니다. RFC에 제공한 태그 키 이름이 리소스에 이미 있는 경우 태그 값은 RFC에 제공한 새 태그 값으로 바뀝니다. 태그 키:값 페어의 총 길이는 256자를 초과할 수 없습니다.

AMS 생성 리소스에 태그를 지정하기 위한 배포 | 고급 스택 구성 요소 | 태그 | 생성(검토 필요) 변경 유형(ct-0176f0n99vcps)과 함께 RFC에 다음 정보를 포함합니다.

1. 관리를 위해 AMS 생성 리소스에 태그를 지정하려는 다중 계정 랜딩 존 또는 단일 계정 랜딩 존 계정의 목록입니다.
2. 필수 태그 키 이름 및 태그 값(필요한 경우). 기본적으로 AMS는 태그 키 이름을 "EnvironmentType"으로 지정하고 태그 값을 "AMSInfrastructure"로 지정할 수 있습니다. 사용자 지정 태그 키 이름 및 태그 값이 필요한 경우 AWS 태그 이름 지정 표준: [태그 지정 모범 사례](#)를 따릅니다.

이러한 리소스는 현재 AMS 인프라 태그 지정에서 지원됩니다.

API Gateway
Amazon CloudFront
Amazon DynamoDB
Amazon EBS
Amazon EC2

```

Amazon OpenSearch Service
Amazon Quantum Ledger Database (QLDB)
Amazon Redshift
Amazon RDS
Amazon S3 (specific buckets only*)
Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
Amazon VPC AWS Certificate Manager AWS CloudFormation AWS CloudTrail AWS CodeBuild
AWS CodePipeline AWS Elastic Beanstalk AWS Lambda AWS Secrets Manager AWS Service
Catalog AWS Systems Manager AWS WAF Regional
Elastic Load Balancing

```

* "arn:aws:s3::awsms-a*-patch-data-*", "arn:aws:s3::ams-a*-log-management-*", "arn:aws:s3::cf-templates-*", "arn:aws:s3::mc-a*", "arn:aws::ams-a*-backup-reports-*", "arn:aws:s3::ams-a*-patch-data-customer-reports-*", "arn:aws:s3::ams-a*-patch-data-raw-n-patch-data-reporting-ams-cfn-drift-remediation-ams-reporting-data-a

AMS 권장 태그

AMS는 지원되는 리소스에 대해 다음 태그를 권장합니다. 별표(*) 태그를 사용하는 것이 좋습니다.

Note

태그를 사용하여 패치 적용을 예약할 수 있습니다. 자세한 내용은 [AMS Advanced Patch Orchestrator: a tag-based patching model](#)을 참조하세요.

AMS 예약 접두사

AMS 리소스 속성은 특정 패턴을 준수해야 합니다. 예를 들어 IAM 인스턴스 프로파일 이름, BackupVault 이름, 태그 이름 등은 AMS 예약 접두사로 시작해서는 안 됩니다. 이러한 예약 접두사는 다음과 같습니다.

```

*/aws_reserved/*
ams-*
/ams/*
ams*
AMS*
Ams*
aws*

```

```

AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion

```

AMS 권장 태그

태그 키	지원되는 값	참고
AppName*	제약이 없습니다.	리소스에 상주하거나 리소스에 액세스해야 하는 애플리케이션을 식별합니다. 이를 통해 AMS와 사용자 간의 추적 및 통신을 용이하게 할 수 있습니다.
AppId*		
EnvironmentType *		개발, 테스트 및 프로덕션 인프라를 리소스의 환경으로 구분합니다.

태그 키	지원되는 값	참고
OwnerTeamEmail *	배포 목록 이메일 주소	리소스를 담당하는 팀의 배포 목록 이메일 주소를 식별합니다. 이메일은 개인 이메일이 아니어야 하며 배포 목록과 같은 익명 이메일이어야 합니다.
ComplianceFramework	무제약	리소스에 적용해야 하는 제어 및 정책을 식별합니다.
CostCenter		리소스와 연결된 비용 센터 또는 사업부를 식별합니다(일반적으로 비용 할당 및 추적).
Customer		여러 고객(AMS 하위 고객)의 리소스를 보유한 AMS 고객이 사용합니다. 관리형 환경의 리소스를 서비스 중인 특정 고객으로 그룹화합니다. 특정 리소스 또는 서비스 그룹에서 특정 클라이언트를 식별합니다.
DataClassification		리소스가 지원하는 특정 데이터 기밀 수준을 식별합니다. 리소스에 적용해야 하는 제어 및 정책을 식별합니다.
HoursOfOperation		리소스를 시작, 중지, 삭제 또는 교체해야 하는 날짜 또는 시간을 식별합니다.
OwnerTeam		리소스를 담당하는 팀을 식별합니다. 리소스를 담당하는 팀과의 커뮤니케이션을 촉진합니다.

태그 키	지원되는 값	참고
Patch Group	여기에는 두 가지 옵션이 있습니다. • AMS Advanced Patch Orchestrator에 설명된 정보, 즉 태그 기반 패치 적용 모델을 사용하여 서비스 요청을 제출할 수 있으며, AMS는 사용자가 제공한 정보를 사용하여 지정된 리소스에 Patch Group를 생성합니다. • 리소스에 Patch Group 태그를 이미 생성한 경우 지원되는 값은 제한되지 않습니다.	자동 패치 유지 관리 기간에 포함할 리소스입니다.
ProjectId	무제약	리소스가 지원하는 프로젝트를 식별합니다.
SupportPriority	기밀성, 무결성 또는 가용성에 대해 가능한 6개의 두문자어 중 하나이며, 두문자어의 순서가 우선 순위입니다. 예를 들어 I.C.A.는 주문이 무결성, 기밀성, 가용성임을 의미합니다. 다른 허용 가능한 값은 C.I.A., C.A.I., I.A.C., A.C.I. 및 A.I.C입니다.	기밀성, 무결성 또는 가용성과 같이 우선해야 하는 지원 유형을 식별합니다.

대량 업데이트 정보 태그 지정

이 참고 사항은 [태그 | 대량 업데이트](#) 및 [태그 | 대량 업데이트\(검토 필요\)](#) 변경 유형 예제 안내와 함께 사용됩니다.

대량 업데이트 태그에 대한 참고 사항:

- 지원되는 서비스:
 - [태그 | 대량 업데이트\(검토 필요\)](#)의 경우: 모두.
 - [태그 | 대량 업데이트](#)의 경우:
 - 오토 스케일링
 - Amazon EC2
 - Elastic Load Balancing
 - Amazon RDS
 - Amazon S3 버킷
- 쉼표로 구분된 값(CSV) 파일을 생성하려면 AWS 콘솔에서 Resource Groups > Tag Editor에 로그인하고 태그를 지정할 리소스를 찾은 다음 CSV 파일로 내보냅니다. 자세한 내용은 [CSV로 결과 내보내기](#)를 참조하세요.

참고: CSV 객체 위치를 제공하려면 S3 미리 서명된 URL을 사용하는 것이 좋습니다.

- 헤더 서비스, 유형 및 식별자가 있는 열이 있어야 합니다. 이러한 열은 필수입니다.
- 열 식별자의 이름을 ID로 바꿉니다.
- Service, Type 및 Identifier(ID로 변경됨) 열의 값은 Resource Groups 아래의 Tag Editor에서 제공하는 것과 같습니다.
- 태그 편집기에서 태그를 지정할 리소스를 사용할 수 없는 경우 식별자(ID로 변경됨) 열에 리소스의 Amazon 리소스 이름(ARN)을 사용하고 서비스 및 유형을 비워 둡니다.
- 추가하거나 수정할 태그의 열 헤더는 Tag: **TagKey** 형식이어야 합니다.
- 삭제할 태그의 열 헤더는 Untag: **TagKey** 형식이어야 합니다.
- 각 행은 리소스에 태그를 지정하거나 태그를 해제하기 위한 것입니다.
- 태그를 리소스에 추가하려면 해당 태그: **TagKey** 열에 태그 값을 지정합니다.
- 리소스에서 태그를 삭제하려면 해당 태그 해제: **TagKey** 열에서 True를 지정합니다.
- Tag: **TagKey** 또는 Untag: **TagKey**를 리소스에 적용할 수 없는 경우 각 열에 대시(-)를 추가하거나 비워 둡니다.

참고: 태그 해제는 태그를 재정의합니다. 태그와 달리 태그 해제는 CSV 파일에 수동으로 추가해야 하므로 태그를 수정하지 않고 제거하려는 의도라고 가정합니다.

- 기준에 맞지 않는 추가 열은 무시됩니다.

Important

Tag Editor 내보내기는 모든 리소스에 대해 모든 태그의 행렬을 채우고 누락된 태그는 '태깅되지 않음' 값으로 채워집니다. 이 내보내기 CSV를 RFC에 대한 입력으로 재사용하면 이전에 누락된 모든 태그가 생성되고 리터럴 값은 '태깅되지 않음'이 됩니다.

Note

태그를 CSV 파일로 내보내는 방법에 대한 자세한 내용은 [태그를 지정할 리소스 찾기 -> CSV로 결과 내보내기를 참조하세요](#).

AWS Managed Services 리소스 스케줄러

AWS Managed Services(AMS) Resource Scheduler를 사용하여 계정에서 AutoScaling 그룹, Amazon EC2 인스턴스 및 RDS 인스턴스의 자동 시작 및 중지를 예약합니다. 이렇게 하면 리소스가 연중무휴로 실행되지 않는 인프라 비용을 줄일 수 있습니다. 이 솔루션은 [의 인스턴스 스케줄러 AWS](#)를 기반으로 구축되지만 AMS 요구 사항에 맞는 추가 기능 및 사용자 지정이 포함되어 있습니다.

Note

기본적으로 AMS Resource Scheduler는 AWS CloudFormation 스택의 일부가 아닌 리소스와 상호 작용하지 않습니다. 리소스는 "stack-", "sc-" 또는 "SC-"로 시작하는 스택의 일부여야 합니다. CloudFormation 스택에 포함되지 않은 리소스를 예약하려면 Resource Scheduler 스택 파라미터를 ScheduleNonStackResources로 업데이트하면 됩니다.

AMS Resource Scheduler는 기간과 일정을 사용합니다.

- 기간은 시작 시간, 종료 시간, 월의 일 등 Resource Scheduler가 실행되는 시간을 정의합니다.

- 일정에는 SSM 유지 관리 기간, 시간대, 최대 절전 모드 설정 등과 같은 추가 구성과 함께 정의된 기간이 포함되며, 구성된 기간 규칙을 고려하여 리소스를 실행해야 하는 시기를 지정합니다.

AMS Resource Scheduler의 자동 변경 유형(CTs).

AMS Resource Scheduler에 사용할 수 있는 설정에 대한 자세한 내용은 [솔루션 구성](#) 요소의 해당 AWS 인스턴스 스케줄러 설명서를 참조하세요. 솔루션의 아키텍처 보기는 [Architecture overview.html](#)의 해당 AWS 인스턴스 스케줄러 설명서를 참조하세요.

AMS Resource Scheduler 배포

AMS Resource Scheduler를 배포하려면 자동 변경 유형(CT) : Deployment | AMS Resource Scheduler | Solution | Deploy(ct-0ywnhc8e5k9z5)를 사용하여 계정에 솔루션을 배포하는 RFC를 생성합니다. RFC가 실행되면 기본 구성의 AMS Resource Scheduler 리소스가 포함된 CloudFormation 스택이 계정에 자동으로 프로비저닝됩니다. Resource Scheduler 변경 유형에 대한 자세한 내용은 [AMS Resource Scheduler](#)를 참조하세요.

Note

AMS Resource Scheduler가 계정에 이미 배포되어 있는지 확인하려면 AWS Lambda 콘솔에서 해당 계정을 확인하고 AMSResourceScheduler 함수를 찾습니다.

계정에 AMS Resource Scheduler를 프로비저닝한 후에는 기본 구성을 검토하고 필요한 경우 기본 설정에 따라 태그 키, 시간대, 예약된 서비스 등과 같은 구성을 사용자 지정하는 것이 좋습니다. 권장 사용자 지정에 대한 자세한 내용은 [AMS Resource Scheduler 사용자 지정](#) 다음 단원을 참조하십시오.

사용자 지정 구성을 만들거나 Resource Scheduler 구성을 확인하려면

AMS Resource Scheduler 사용자 지정

업데이트 AMS Resource Scheduler 변경 유형을 사용하여 AMS Resource Scheduler의 다음 속성을 사용자 지정하는 것이 좋습니다. [AMS Resource Scheduler](#)를 참조하세요.

- 태그 이름: Resource Scheduler가 인스턴스 일정을 리소스와 연결하는 데 사용할 태그의 이름입니다. 기본값은 일정입니다.
- 예약된 서비스: Resource Scheduler가 관리할 수 있는 심표로 구분된 서비스 목록입니다. 기본값은 "ec2,rds,autoscaling"입니다. 유효한 값은 "ec2", "rds" 및 "autoscaling"입니다.
- 기본 시간대: Resource Scheduler에서 사용할 기본 시간대를 지정합니다. 기본값은 UTC입니다.

- CMK 사용: Resource Scheduler에 권한을 부여할 수 있는 쉼표로 구분된 Amazon KMS 고객 관리형 키(CMK) ARNs.
- LicenseManager 사용: Resource Scheduler에 대한 AWS Licence Manager ARNs 목록을 쉼표로 구분하여 권한을 부여할 수 있습니다.

Note

AMS는 계정에서 AMS Resource Scheduler를 최신 상태로 유지하기 위해 기능 및 수정 사항을 릴리스할 수 있습니다. 이 경우 AMS Resource Scheduler에 대한 사용자 지정은 유지됩니다.

AMS Resource Scheduler 사용

솔루션을 배포한 후 AMS Resource Scheduler를 구성하려면 자동화된 Resource Scheduler CTs를 사용하여 AMS Resource Scheduler 기간(Resource Scheduler가 실행되는 시간) 및 일정(구성된 기간 및 기타 옵션)을 생성, 삭제, 업데이트 및 설명(상세 정보 가져오기)합니다. AMS Resource Scheduler 변경 유형을 사용하는 예는 [AMS Resource Scheduler](#)를 참조하세요.

AMS Resource Scheduler에서 관리할 리소스를 선택하려면 배포 및 일정 생성 후 AMS 태그 CTs 생성을 사용하여 Auto Scaling 그룹, Amazon RDS 스택 및 Amazon EC2 리소스에 배포 중에 제공한 태그 키로 태그를 지정하고 정의된 일정을 태그 값으로 지정합니다. 리소스에 태그를 지정하면 정의된 Resource Scheduler 일정에 따라 리소스가 시작 또는 중지되도록 예약됩니다.

AMS Resource Scheduler를 사용하는 데 드는 추가 비용은 없습니다. 그러나 솔루션은 여러를 사용 AWS 서비스 하며 이러한 리소스가 사용될 때 요금이 부과됩니다. 자세한 내용은 [아키텍처 개요](#)를 참조하세요.

AMS Resource Scheduler를 오프아웃하려면

- 임시 오프아웃 또는 비활성화의 경우: 자동 관리 | AMS 리소스 스케줄러 | 상태 | 변경 유형 비활성화(ct-14v49adibs4db)를 사용하여 RFC 제출
- 영구 제거의 경우: 관리 제출 | 기타 | 기타 | 업데이트(검토 필요)(ct-0xdawir96cy7k) Resource Scheduler 릴리스 자동화 시스템에서 제거를 요청하는 RFC

AMS Resource Scheduler 비용 예측기

비용 절감을 추적하기 위해 AMS Resource Scheduler는 스케줄러에서 관리하는 Amazon EC2 및 RDS 리소스의 예상 비용 절감을 시간당 계산하는 구성 요소를 제공합니다. 그러면이 비용 절감 데이터가

CloudWatch 지표(AMS/ResourceScheduler)로 게시되어 이를 추적하는 데 도움이 됩니다. 비용 절감 예측기는 인스턴스 실행 시간에 대한 절감액만 추정합니다. 리소스와 관련된 데이터 전송 비용과 같은 다른 비용은 고려하지 않습니다.

비용 절감 예측기는 Resource Scheduler에서 활성화됩니다. 시간당 실행되며에서 비용 및 사용량 데이터를 검색합니다 AWS Cost Explorer. 해당 데이터에서 각 인스턴스 유형에 대한 시간당 평균 비용을 계산한 다음 예약 없이 실행되는 경우 하루 종일 비용을 프로젝트합니다. 비용 절감은 예상 비용과 지정된 날짜 동안 Cost Explorer에서 실제로 보고된 비용 간의 차이입니다.

예를 들어 인스턴스 A가 오전 9시부터 오후 5시까지 실행되도록 Resource Scheduler로 구성된 경우 해당 날짜의 8시간입니다. Cost Explorer는 비용을 1 USD로, 사용량을 8로 보고합니다. 따라서 시간당 평균 비용은 0.125 USD입니다. 인스턴스가 Resource Scheduler로 예약되지 않은 경우 인스턴스는 해당 날짜에 24시간 실행됩니다. 이 경우 비용은 $24 \times 0.125 = 3$ USD였습니다. Resource Scheduler를 사용하면 2 USD의 비용 절감을 달성할 수 있습니다.

비용 절감 예측기가 Cost Explorer에서 Resource Scheduler에서 관리하는 리소스에 대해서만 비용 및 사용량을 검색하려면 Resource Scheduler가 리소스를 대상으로 지정하는 데 사용하는 태그 키를 결제 대시보드에서 비용 할당 태그로 활성화해야 합니다. 계정이 조직에 속한 경우 조직의 관리 계정에서 태그 키를 활성화해야 합니다. 이에 대한 자세한 내용은 [사용자 정의 비용 할당 태그 및 사용자 정의 비용 할당 태그 활성화를 참조하세요.](#)

태그 키가 비용 할당 태그로 활성화되면 AWS 청구는 Resource Scheduler에서 관리하는 리소스의 비용 및 사용량을 추적하기 시작하고 해당 데이터를 사용할 수 있게 되면 비용 절감 예측기는 비용 절감을 계산하고 CloudWatch의 AMS/ResourceScheduler 지표 네임스페이스에 데이터를 게시하기 시작합니다.

비용 예측기 팁

Cost Savings Estimator는 계산 시 예약 인스턴스, 절감형 플랜 등과 같은 할인을 허용하지 않습니다. 예측기는 Cost Explorer에서 사용 비용을 받아 리소스의 시간당 평균 비용을 계산합니다. 자세한 내용은 [AWS 비용 데이터세트 이해: 치트 시트를 참조하세요.](#)

비용 절감 예측기가 Cost Explorer에서 Resource Scheduler에서 관리하는 리소스에 대해서만 비용 및 사용량을 검색하려면 Resource Scheduler가 리소스를 대상으로 지정하는 데 사용하는 태그 키를 결제 대시보드에서 비용 할당 태그로 활성화해야 합니다. 계정이 조직에 속한 경우 조직의 관리 계정에서 태그 키를 활성화해야 합니다. 이에 대한 자세한 내용은 [사용자 정의 비용 할당 태그를 참조하세요.](#) 비용 할당 태그가 활성화되지 않은 경우 예측기는 절감액을 계산하고 활성화된 경우에도 지표를 게시할 수 없습니다.

AMS Resource Scheduler 모범 사례

Amazon EC2 인스턴스 예약

- 인스턴스 종료 동작은 `stop` 아닌 `terminate` 로 설정해야 합니다. 이는 AMS Amazon EC2 자동 변경 유형 생성(ct-14027q0sjyt1h)으로 생성된 인스턴스의 `stop` 경우로 사전 설정되며 속성을 `stop` 로 설정하여 AWS CloudFormation 수집으로 생성된 Amazon EC2 인스턴스의 경우 `InstanceInitiatedShutdownBehavior`로 설정할 수 있습니다. `stop` 인스턴스 종료 동작이 설정된 경우 Resource Scheduler가 종료하고 스케줄러가 다시 시작할 수 없을 때 `terminate` 인스턴스가 종료됩니다.
- Auto Scaling 그룹의 일부인 Amazon EC2 인스턴스는 태그가 지정된 경우에도 AMS Resource Scheduler에서 개별적으로 처리되지 않습니다.
- 대상 인스턴스 루트 볼륨이 KMS 고객 마스터 키(CMK)로 암호화된 경우 스케줄러가 해당 인스턴스를 시작할 수 있도록 Resource Scheduler IAM 역할에 추가 `kms:CreateGrant` 권한을 추가해야 합니다. 보안 향상을 위해 이 권한은 기본적으로 역할에 추가되지 않습니다. 이 권한이 필요한 경우 Management | AMS Resource Scheduler | Solution | Update change type을 사용하여 RFC를 제출하고 KMS CMKs의 심포로 구분된 ARNs 목록을 지정합니다.

Auto Scaling 그룹 예약

- AMS Resource Scheduler는 오토 스케일링의 개별 인스턴스가 아닌 Auto Scaling의 오토 스케일링을 시작하거나 중지합니다. 즉, 스케줄러는 Auto Scaling 그룹의 크기를 복원하거나(시작) 크기를 0(중지)으로 설정합니다.
- AutoScaling 그룹에 그룹 내 인스턴스가 아닌 지정된 태그로 태그를 지정합니다.
- 중지하는 동안 AMS Resource Scheduler는 Auto Scaling 그룹의 최소, 원하는 및 최대 용량 값을 저장하고 최소 및 원하는 용량을 0으로 설정합니다. 시작하는 동안 스케줄러는 Auto Scaling 그룹 크기를 중지하는 동안과 동일하게 복원합니다. 따라서 Auto Scaling 그룹 인스턴스는 인스턴스의 종료 및 다시 시작이 Auto Scaling 그룹에서 실행되는 애플리케이션에 영향을 주지 않도록 적절한 용량 구성을 사용해야 합니다.
- 실행 기간 동안 Auto Scaling 그룹이 수정된 경우(최소 또는 최대 용량) 스케줄러는 새 Auto Scaling 그룹 크기를 저장하고 중지 일정이 끝날 때 그룹을 복원할 때 사용합니다.

Amazon RDS 인스턴스 예약

- 스케줄러는 RDS 인스턴스를 중지하기 전에 스냅샷을 생성할 수 있습니다(Aurora DB 클러스터에는 적용되지 않음). 이 기능은 기본적으로 RDS 인스턴스 스냅샷 생성 AWS CloudFormation 템플릿 파

라미터를 true로 설정하여 활성화됩니다. 스냅샷은 다음에 Amazon RDS 인스턴스가 중지되고 새 스냅샷이 생성될 때까지 유지됩니다.

스케줄러는 클러스터 또는 Amazon RDS Aurora 데이터베이스의 일부이거나 다중 가용 영역(다중 AZ) 구성에 있는 Amazon RDS 인스턴스를 시작/중지할 수 있습니다. 그러나 스케줄러가 Amazon RDS 인스턴스, 특히 다중 AZ 인스턴스를 중지할 수 없는 경우 Amazon RDS 제한을 확인합니다. Aurora 클러스터의 시작 또는 중지를 예약하려면 Aurora 클러스터 예약 템플릿 파라미터(기본값은 true)를 사용합니다. Aurora 클러스터(클러스터 내의 개별 인스턴스 아님)에는 초기 구성 중에 정의된 태그 키와 해당 클러스터를 예약하기 위한 태그 값으로 일정 이름을 지정해야 합니다.

모든 Amazon RDS 인스턴스에는 시스템 변경 사항이 적용되는 주간 유지 관리 기간이 있습니다. 유지 관리 기간 동안 Amazon RDS는 유지 관리를 적용하기 위해 7일 이상 중지된 인스턴스를 자동으로 시작합니다. 유지 관리 이벤트가 완료되면 Amazon RDS가 인스턴스를 중지하지 않습니다.

스케줄러를 사용하면 Amazon RDS 인스턴스의 기본 유지 관리 기간을 일정에 실행 기간으로 추가할지 여부를 지정할 수 있습니다. 다른 실행 기간에서 인스턴스를 실행해야 한다고 지정하지 않고 유지 관리 이벤트가 완료된 경우 솔루션은 유지 관리 기간 시작 시 인스턴스를 시작하고 유지 관리 기간 종료 시 인스턴스를 중지합니다.

유지 관리 기간이 끝날 때까지 유지 관리 이벤트가 완료되지 않으면 유지 관리 이벤트가 완료된 후 예약 간격까지 인스턴스가 실행됩니다.

Note

스케줄러는 리소스가 시작되거나 중지되었는지 확인하지 않습니다. API를 호출하고 계속 진행합니다. API 호출이 실패하면 조사를 위해 오류를 기록합니다.

AWS Systems Manager AMS Advanced의

AWS Systems Manager 문서(SSM 문서)는 Systems Manager가 AWS 리소스에서 수행하는 작업을 정의합니다. Systems Manager에는 런타임 시 파라미터를 지정하여 사용할 수 있는 사전 구성된 문서가 12개 이상 포함되어 있습니다. 문서는 JavaScript Object Notation(JSON) 또는 YAML을 사용하며 사용자가 지정하는 단계와 파라미터를 포함합니다.

AWS Managed Services(AMS)는 SSM 문서의 신뢰할 수 있는 게시자입니다. AMS가 소유한 SSM 문서는 온보딩된 AMS 계정과만 공유되며, 항상 예약된 접두사(AWSManagedServices-*)로 시작하고 소유한 Systems Manager 콘솔에 표시됩니다 AWS. SSM 문서 개발 및 게시를 위한 AMS 프로세스는

AWS 모범 사례를 따르며 문서 수명 주기 전반에 걸쳐 여러 피어 검토가 필요합니다. SSM 문서 공유 AWS 모범 사례에 대한 자세한 내용은 [공유 SSM 문서 모범 사례를 참조하세요](#).

사용 가능한 AMS Advanced SSM 문서

AMS Advanced SSM 문서는 AMS Advanced 고객만 사용할 수 있으며 계정 운영을 위한 운영 워크플로를 자동화하는 데 사용됩니다.

에서 사용 가능한 AMS Advanced SSM 문서를 보려면 AWS Management Console:

1. [AWS Systems Manager 콘솔](#)에서 Systems Manager콘솔을 엽니다.
2. 나와 공유를 선택합니다.
3. 검색 창에서 문서 이름 접두사를 기준으로 필터링한 다음 같음을 기준으로 값을 AWSManagedServices-로 설정합니다.

AWS CLI 지침은 [공유 SSM 문서 사용](#)을 참조하세요.

AMS Advanced SSM 문서 버전

SSM 문서는 버전 관리를 지원합니다. AMS Advanced SSM 문서는 고객의 계정에서 수정할 수 없으며 다시 공유할 수 없습니다. 계정을 운영하기 위해 AMS Advanced에서 중앙에서 관리하고 유지 관리합니다.

버전 번호는 특정에서 각 문서 업데이트에 따라 증가합니다 AWS 리전. 새 리전을 사용할 수 있게 되면 두 리전의 동일한 문서 콘텐츠의 버전 번호가 다를 수 있습니다. 이는 일반적이며 동작이 다르다는 의미는 아닙니다. 두 개의 AMS Advanced SSM 문서를 비교하려면 해시를 AWS CLI와 비교하는 것이 좋습니다.

```
aws ssm describe-document \
  --name AWSManagedServices-DOCUMENTNAME \
  --output text --query "Document.Hash"
```

해시가 일치하면 두 개의 SSM 문서가 동일합니다.

AMS의 Systems Manager 요금

AMS Advanced SSM 문서 액세스와 관련된 비용은 없습니다. 런타임 비용은 SSM 문서 유형, 단계 및 런타임 기간에 따라 달라집니다. 자세한 내용은 [AWS Systems Manager 요금](#)을 참조하세요.

AMS 계정 오프보드

AMS는 단일 계정 랜딩 존 및 다중 계정 랜딩 존 계정에 대한 오프보딩 지원을 제공합니다.

AMS는 종속성에 영향을 주지 않도록 오프보딩 중에 AMIs를 공유 해제하지 않습니다. 계정에서 AMS AMIs 제거하려면 `cancel-image-launch-permission` API를 사용하여 특정 AMIs를 숨길 수 있습니다. 예를 들어 아래 스크립트를 사용하여 이전에 계정과 공유된 모든 AMS AMIs를 숨길 수 있습니다.

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --query 'Images[].ImageId' --output text) ;
do
    aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

스크립트가 오류 없이 실행되려면 AWS CLI v2가 설치되어 있어야 합니다. AWS CLI 설치 단계는 [AWS CLI의 최신 버전 설치 또는 업데이트를 참조하세요](#). `cancel-image-launch-permission` 명령에 대한 자세한 내용은 섹션을 참조하세요 [cancel-image-launch-permission](#).

Note

서비스 종료 날짜는 30일 필수 종료 알림 기간이 끝나는 달의 마지막 날입니다. 필수 종료 알림 기간이 해당 월의 20일 이후인 경우 서비스 종료 날짜는 다음 달의 마지막 날입니다. 다음은 종료 날짜에 대한 예제 시나리오입니다.

- 해지 알림이 4월 12일에 제공된 경우 30일 알림은 5월 12일에 종료됩니다. 서비스 종료 날짜는 5월 31일입니다.
- 종료 알림이 4월 29일에 제공된 경우 30일 알림은 5월 29일에 종료됩니다. 서비스 종료 날짜는 6월 30일입니다.

주제

- [AMS 단일 계정 랜딩 존 계정에서 오프보드](#)
- [AMS 다중 계정 랜딩 존 계정에서 오프보드](#)

AMS 단일 계정 랜딩 존 계정에서 오프보드

AMS는 AMS 종료 전 30일 이내에 오프보딩 지원을 제공합니다.

이러한 지원이 제공되려면 최소 7일 전에 오프보딩 지원을 요청해야 합니다. 오프보딩 지원은 두 가지 형태로 제공될 수 있습니다.

- 제어 인계: AMS는 모든 AMS 관리형 애플리케이션의 액세스 자격 증명과 함께 계정 제어를 다시 전송합니다. 또는
- 계정 해지를 위한 리소스 종료: AMS는 AMS 관리형 환경의 모든 데이터를 삭제하고 계정의 활성 리소스를 프로비저닝 해제합니다. 오프보딩 요청을 제출할 때 고객은 AMS에 다음을 요청할 수 있습니다.
 - Amazon S3 버킷에 저장된 데이터 객체(로그 포함) 삭제 또는 유지
 - Amazon S3 버킷 제거 또는 유지
 - AWS Backup 복원 지점 제거 또는 유지

Important

오프보딩을 초기화하기 전에 다른 모든 특정 요청(타당성에 따라 다름)을 AMS에 전달해야 합니다.

선택적 사전 조건(필요한 경우):

Note

오프보딩 요청 전에 고객은 AWS Snowball Edge 또는와 AWS 인터페이스하는 다른 미디어를 사용하여 기존 형식으로 데이터를 전송하기 위해 AMS 지원을 요청할 수 있습니다.

데이터 백업 외에도 오프보딩 지원의 일환으로 다음과 같은 고객 데이터를 제공할 수 있습니다.

- 로그를 포함하여 스토리지 서비스에 저장된 데이터
- 고객별 변경 유형 스키마
- 변경 유형 스키마에 대한 CloudFormation 템플릿

AMS 종료 시 오프보딩 활동이 완료되지 않은 경우 보류 중인 활동을 완료할 수 있도록 계정(들)의 컨트롤을 인계합니다.

함수	제거된 항목	영향	필요한 작업
모니터링, 로깅, 알림	AMS 모니터링 제거됨 MMS(관리형 모니터링 시스템) 구독 취소 Resource Tagger 및 Alarm Manager 제거됨 기존 CloudWatch 알림은 기존 리소스에 남아 있습니다. GuardDuty 및 Macie: 소유권이 되돌림	AMS는 더 이상 리소스 및 환경에 대한 액세스 또는 가시성이 없습니다.	제거 및 구독 취소된 서비스에 대한 비상 상황은 사용자가 소유합니다.
백업 관리	AWS Backup 서비스를 계속 사용할 수 있지만 AMS Backup 자동화는 제거됩니다. 백업 볼트와 데이터는 삭제 요청되지 않는 한 보존됩니다.	AMS는 더 이상 백업 작업을 모니터링하거나 인시던트 발생 시 복원 작업을 수행하지 않습니다. 경고 및 알림이 비활성화됩니다. IAM 백업 역할 및 KMS 키를 삭제하면 AMS 백업이 작동하지 않습니다.	AMS 백업 계획을 재구성해야 합니다. 모든 모니터링 및 수정 소유권이 반환됩니다.
서비스 관리를 위한 AMS 자동화	AMS에서 선별한 AWS SSM 자동화 런북, Amazon Simple Notification Service(SNS) 및 AWS Lambda 함수는 더 이상 사용할 수 없습니다.	계정에 대한 AMS 액세스 권한이 없습니다. 모든 자동화가 비활성화되었습니다.	필요한 경우 SSM, SNS 및 Lambda 함수를 포함한 모든 자동화를 다시 생성해야 합니다.

함수	제거된 항목	영향	필요한 작업
규정 준수	모든 GuardDuty 및 AWS Config 규칙에 대한 AMS 가시성 및 모니터링은 제거되었지만 이러한 규칙은 계정에 남아 있습니다.	Amazon GuardDuty 및 AWS Config 규칙의 모든 모니터링, 보고 및 수정은 더 이상 AMS에서 관리하지 않습니다.	사용자가 수입할 모든 보안 및 규정 준수 도구에 대한 모니터링 및 문제 해결.
온인스턴스 에이전트	EC2 인스턴스에 필요한 에이전트를 설치하기 위한 Resource Scheduler, Resource Tagger 또는 자동 인스턴스 구성에 대한 액세스 권한이 제거됩니다.	인스턴스의 CloudWatch 및 SSM 에이전트는 기존 구성과 함께 그대로 유지되지만 AMS는 더 이상 이러한 구성을 지원하지 않습니다.	태그 지정 및 온인스턴스 CloudWatch 및 SSM 에이전트 구성을 관리합니다.
패치 및 보고 인프라	AMS는 더 이상 패치 전후 활동을 관리하지 않으며 이러한 서비스에 대한 액세스 및 가시성이 제거됩니다.	AMS는 더 이상 패치 적용 전에 인스턴스의 스냅샷을 생성하지 않고, 더 이상 패치 설치를 설치 및 모니터링하지 않으며, 더 이상 결과를 알리지 않습니다. 보고서 및 “감사” S3 버킷은 요청 시 계정에 남아 있습니다. AMS는 더 이상 서비스 지표 보고서를 생성하지 않습니다.	과거에 생성된 패치 기준 및 스냅샷은 유지됩니다. 또한 패치 유지 관리 기간의 구성은 유지되지만 패치는 더 이상 AMS에 의해 설치되거나 수정되지 않습니다. 인프라 운영 지표에 대한 모든 보고는 이제 사용자의 책임입니다.

합수	제거된 항목	영향	필요한 작업
프로세스 관리	모든 계정은 서비스 요청, 문제, 변경, 관리를 포함하여 인시던트에 대해 제공된 서비스 관리에서 오프보딩됩니다.	인시던트 및 서비스 요청을 통해 AMS에 의해 이전에 해결된 모든 서비스 중단과 환경에 대한 변경 사항 및 근본 원인 조사는 AMS에 의해 더 오래 관리됩니다.	모든 프로세스 관리의 전체 소유권을 다시 획득합니다.

AMS 다중 계정 랜딩 존 계정에서 오프보드

AMS Advanced 다중 AWS 계정 랜딩 존에서 오프보딩할 수 있는 두 가지 유형의 계정이 있습니다.

- 애플리케이션 계정
- 코어 계정

AMS 다중 계정 랜딩 존에서 모든 계정을 오프보드하려면 코어 계정을 오프보드하기 전에 모든 애플리케이션 계정을 오프보드해야 합니다.

오프보딩된 애플리케이션 또는 코어 계정에서 워크로드를 인수하고 계속 운영하려면 AMS 계정 팀과 함께이 설명서를 검토해야 합니다. 이 설명서에서는 오프보드 프로세스 중에 AMS가 수행하는 변경 사항을 간략하게 설명합니다.

오프보딩된 계정의 지속적인 운영을 위해 완료해야 할 작업

AMS 다중 계정 랜딩 존에서 오프보딩한 계정을 계속 운영하려면 다음 작업이 필요합니다.

- 개발자 모드 켜기: 계정에 대한 추가 권한을 얻으려면 AMS에서 애플리케이션 계정을 오프보드하기 전에 개발자 모드를 켭니다. 개발자 모드를 켜면 오프보딩을 준비하는 데 필요한 사항을 더 쉽게 변경할 수 있습니다. AMS 인프라 리소스를 제거하거나 수정하지 마세요. AMS 인프라 리소스를 삭제하면 AMS가 계정을 성공적으로 오프보드하지 못할 수 있습니다. 개발자 모드를 활성화하는 방법에 대한 자세한 내용은 [섹션을 참조하세요](#) [AMS Advanced Developer 모드 시작하기](#).

개발자 모드를 켜 후 오프보딩을 준비하는 데 필요한 변경 사항을 완료할 수 없는 경우 AMS 계정 팀에 문의하여 요구 사항을 논의하세요.

- EC2 스택 액세스를 위한 대체 방법 선택: AMS에서 애플리케이션 계정을 오프보드한 후에는 RFCs 사용하여 스택 리소스에 액세스할 수 없습니다. 를 검토한 [오프보딩 변경 사항](#) 다음 스택에 대한 액세스를 유지할 대체 액세스 방법을 선택합니다. 자세한 내용은 [대체 액세스](#) 단원을 참조하십시오.

AMS 애플리케이션 계정 오프보드

다중 계정 랜딩 존 환경에서 애플리케이션 계정을 오프보딩하려면 각 계정에 대해 다음 단계를 완료합니다.

1. 계정에 열려 있는 RFCs가 없는지 확인합니다. 자세한 내용은 [RFCs 생성, 복제, 업데이트, 찾기 및 취소](#) 단원을 참조하십시오.
2. 계정의 기본 또는 루트 사용자 이메일 주소에 액세스할 수 있는지 확인합니다.
3. 애플리케이션 계정에서 [애플리케이션 계정 | 오프보딩 확인](#)(ct-2wlfo2jxj2rkj) 변경 유형을 사용하여 RFC를 제출합니다. RFC에서 오프보드할 애플리케이션 계정을 지정합니다.
4. 관리 계정에서 [관리 계정 | 오프보드 애플리케이션 계정](#)(ct-0vdiy51oyrh) 변경 유형을 사용하여 RFC를 제출합니다. RFC에서 오프보드할 애플리케이션 계정을 지정합니다. 또한 랜딩 존에 대한 전송 게이트웨이 연결을 삭제하거나 유지할지 여부를 지정합니다.
5. AMS 결제가 중지되었는지 확인하려면 계정을 오프보딩했음을 CSDM에 알립니다.

애플리케이션 계정이 오프보딩된 후 다음이 발생합니다.

- 모든 구성 요소는 AMS 서비스에서 연결 해제되지만 생성된 리소스는 계정에 남아 있습니다. AMS 오프보딩된 계정을 유지하거나 달도록 선택할 수 있습니다.
- 코어 계정 및 기타 나머지 애플리케이션 계정은 애플리케이션 계정이 오프보딩된 후 정상적으로 작동합니다.
- AMS 결제는 중지되지만 계정을 해지할 때까지 AWS 결제는 중지되지 않습니다. 자세한 내용은 [계정을 해지하기 전에 알아야 할 사항을 참조하세요](#).
- 계정이 해지되면 90일 suspended 동안 조직에 상태가 표시됩니다. 90일이 지나면 해지된 계정이 영구적으로 제거되고 조직에 더 이상 표시되지 않습니다.
- 계정이 해지된 후에도 90일 지원 동안 로그인하여 지원 사례 또는 연락처를 제출할 수 있습니다.
- 90일이 지나면 계정에 남아 있는 모든 콘텐츠가 영구적으로 삭제되고 나머지 AWS 서비스가 종료됩니다.

애플리케이션 계정 오프보딩 FAQ

Q: 연합된 IAM 역할을 사용하여 AMS 다중 계정 랜딩 존에서 오프보딩한 애플리케이션 계정에 계속 액세스할 수 있나요?

예. AMS에서 생성한 [기본 AWS Identity and Access Management \(IAM\) 역할](#)은 AMS 오프보딩 후에도 계정에서 계속 사용할 수 있습니다. 그러나 이러한 역할 및 정책은 AMS 액세스 관리와 함께 사용하도록 설계되었습니다. 사용자에게 필요한 액세스 권한을 제공하려면 자체 IAM 리소스를 배포해야 할 수 있습니다.

Q: AMS 다중 계정 랜딩 존에서 오프보딩한 애플리케이션 계정에 대한 전체 액세스 권한을 얻으려면 어떻게 해야 합니까?

오프보딩된 애플리케이션 계정은 AWS Organizations 계정 구조의 더 이상 사용되지 않는 조직 단위(OU)로 이동합니다. 이 이동은 이전에 루트 사용자 액세스를 차단한 SCP 액세스 제한을 해제합니다. 루트 사용자 자격 증명을 재설정하는 방법에 대한 자세한 내용은 [분실했거나 잊어버린 루트 사용자 암호 재설정을 참조하세요](#).

Q: 애플리케이션 계정 오프보딩 중에 어떤 변경 사항이 적용되나요?

서비스가 계정을 오프보딩할 때 AMS가 수행하는 작업에 대한 자세한 내용은 [섹션을 참조하세요](#) [오프보딩 변경 사항](#).

Q: 전송 게이트웨이에서 분리하지 않고 애플리케이션 계정을 오프보딩할 수 있나요?

예. [관리 계정 | 오프보딩 애플리케이션 계정](#)(ct-0vdiy51oyrh) 변경 유형을 사용하여 RFC를 제출하고 DeleteTransitGatewayAttachment 파라미터를 로 지정합니다False.

Q: 애플리케이션 계정을 오프보딩하는 데 얼마나 걸리나요?

[관리 계정 | 오프보딩 애플리케이션 계정](#)(ct-0vdiy51oyrh) 변경 유형을 사용하면 RFCs 1시간 이내에 완료됩니다.

Q: 오프보딩된 계정을 달아야 하나요?

아니요. AMS 오프보딩 후 계정을 해지할 필요는 없습니다. 오프보딩 프로세스 중에 AMS는 AWS 계정의 액세스 및 관리를 제거하지만 계정과 계정 내 리소스는 유지됩니다. AMS 오프보딩 후 AWS 계정 및 리소스를 관리하고 유지 관리하는 것은 전적으로 사용자의 책임입니다. AMS는 오프보딩 프로세스가 완료된 후 계정에서 발생할 수 있는 문제, 인시던트 또는 서비스 중단에 대해 책임을 지지 않습니다. 자세한 내용은 [AWS 계정을 해지하려면 어떻게 해야 하나요?](#)를 참조하세요.

Q: 계정 해지 요청을 제출하면 기존 리소스가 모두 즉시 삭제되나요?

아니요. 계정 폐쇄는 리소스를 종료하지 않습니다. 계정의 리소스는 해지 요청 후 90일이 지나면 자동으로 종료됩니다. AMS 결제는 중지되지만 계정을 해지할 때까지 AWS 리소스 결제는 중지되지 않습니다. 자세한 내용은 [계정을 해지하기 전에 알아야 할 사항을 참조하세요](#).

Q: 애플리케이션 계정의 오프보딩을 예약할 수 있나요?

예. RFCs가 특정 시간에 실행되도록 예약할 수 있습니다. 그러나 관리 [계정 | 오프보드 애플리케이션 계정](#) RFC를 예약하려면 먼저 [애플리케이션 계정 | 오프보딩](#) RFC 확인을 완료해야 합니다. 자세한 내용은 [RFC 예약](#)을 참조하세요.

애플리케이션 계정 오프보딩 RACI

- R: 책임 당사자. 나열된 작업을 완료할 책임이 있는 당사자입니다.
- A: 책임 당사자. 완료된 작업을 승인하는 당사자입니다.
- C: 상담 당사자. 일반적으로 주제 전문가로서 의견을 구하고 양자 통신이 이루어지는 당사자입니다.
- I: 정보 당사자. 종종 작업 또는 결과물 완료 시에만 진행 상황에 대한 정보를 받는 당사자입니다.

활동	Custom	AWS Managed Services(AMS)
사전 조건		
오프보딩할 각 AWS 계정 ID의 루트 이메일 주소에 대한 액세스 확인	R	C
권장 고객 작업에 대한 AMS 설명서 검토 및 AMS 오프보딩을 위한 계정 준비	R	C
필요한 경우 RFC를 제출하여 개발자 모드가 AMS 오프보딩을 위한 계정을 준비할 수 있도록 합니다.	R	정보
필요한 경우 EC2 스택 액세스를 위한 대체 방법을 선택합니다.	R	정보
오프보딩		

활동	Custom	AWS Managed Services(AMS)
RFCs 제출하여 애플리케이션 계정의 오프보딩 확인 및 요청	R	정보
애플리케이션 계정에서 AMS 구성 요소 오프보드	정보	R
AMS CSDM에 오프보딩된 계정 알림으로 AMS 결제 중지	R	정보
오프보딩 후		
루트 사용자 계정 암호 재설정 및 오프보딩된 계정의 루트 액세스 확인	R	C
계정을 닫거나 AMS 오프보딩 설명서의 권장 고객 작업에 대한 AMS 지침에 따라 계정을 계속 운영합니다.	R	C

코어 계정 오프보드

다중 계정 랜딩 존 코어 계정을 오프보딩하려면 다음 단계를 완료하세요.

1. 랜딩 존의 모든 애플리케이션 계정이 AMS에서 오프보딩되었는지 확인합니다.
2. 계정에 열려 있는 RFCs가 없는지 확인합니다. 자세한 내용은 [RFCs 생성, 복제, 업데이트, 찾기 및 취소](#) 단원을 참조하십시오.
3. 모든 코어 계정의 기본 또는 루트 사용자 이메일 주소에 액세스할 수 있는지 확인합니다. 자세한 내용은 [다중 계정 랜딩 존 계정](#) 단원을 참조하십시오.
4. 관리 계정의 기본 또는 루트 사용자 전화번호에 액세스할 수 있는지 확인합니다. AWSManagedServicesBillingRole IAM 역할을 사용하여 전화번호를 업데이트합니다. 자세한 내용은 [내 계정과 연결된 전화번호를 업데이트하려면 어떻게 해야 하나요?](#)를 참조하세요 [AWS](#).
5. AMS 랜딩 존 관리 계정에 로그인하고 AMS 서비스 요청을 제출합니다. 서비스 요청에서 전체 랜딩 존을 오프보딩하도록 지정합니다.

코어 계정이 오프보딩된 후 다음이 발생합니다.

- 모든 구성 요소는 AMS 서비스에서 연결 해제되지만 일부 AWS 리소스는 계정에 남아 있습니다. AMS 오프보딩된 코어 계정을 유지하거나 닫도록 선택할 수 있습니다.
- AMS 결제는 중지되지만 계정을 해지할 때까지 AWS 결제는 중지되지 않습니다. 자세한 내용은 [계정을 해지하기 전에 알아야 할 사항을 참조하세요](#).
- 계정이 해지되면 90일 동안 조직에 suspended 상태가 표시됩니다. 90일이 지나면 해지된 멤버 계정이 영구적으로 제거되고 조직에 더 이상 표시되지 않습니다.
- 계정이 해지된 후에도 90일 지원 동안 로그인하여 지원 사례 또는 연락처를 제출할 수 있습니다.
- 계정이 90일 동안 해지되면 계정에 남아 있는 모든 콘텐츠가 영구적으로 삭제되고 나머지 AWS 서비스가 종료됩니다.

코어 계정 오프보딩 FAQ

Q: 페더레이션 IAM 역할을 사용하여 오프보딩된 코어 계정에 계속 액세스할 수 있나요?

예. AMS에서 생성한 [기본 AWS Identity and Access Management \(IAM\) 역할](#)은 오프보딩된 계정에서 계속 사용할 수 있습니다. 그러나 이러한 역할 및 정책은 AMS 액세스 관리와 함께 사용하도록 설계되었습니다. 사용자에게 필요한 액세스 권한을 제공하려면 자체 IAM 리소스를 배포해야 할 수 있습니다.

Q: AMS 다중 [계정 랜딩 존에서 오프보딩한 후 관리, 공유 서비스, 네트워킹 또는 기타 비애플리케이션 MALZ](#) 계정에 대한 전체 액세스 권한을 얻으려면 어떻게 해야 합니까?

오프보딩 후 [분실하거나 잊어버린 루트 사용자 암호 재설정](#)의 지침에 따라 기본(루트) 사용자 자격 증명을 사용하여 관리 계정 이외의 코어 계정에 액세스합니다. 다른 계정 유형과 달리 관리 계정은 사용을 방지하기 위해 루트 사용자와 연결된 액세스할 수 없는 다중 인증(MFA) 디바이스를 유지합니다. 루트 액세스를 다시 얻으려면 [손실된 MFA 디바이스 복구 프로세스](#)를 따라야 합니다.

Q: 코어 계정 오프보딩 중에 어떤 변경 사항이 적용되나요?

서비스가 계정을 오프보딩할 때 AMS가 수행하는 작업에 대한 자세한 내용은 [섹션을 참조하세요](#) [오프보딩 변경 사항](#).

Q: 코어 계정 오프보딩을 완료하는 데 얼마나 걸리나요?

코어 계정 오프보딩 프로세스는 일반적으로 완료하는 데 최대 30일이 걸립니다. 그러나 필요한 모든 단계를 올바르게 완료하려면 오프보딩이 시작되기 최소 7일 전에 오프보딩 요청을 시작해야 합니다. 쉽게 전환할 수 있도록 미리 계획을 세우고 오프보딩 요청을 미리 제출하세요.

Q: AMS 오프보딩 후 공유 구성 요소를 관리하려면 어떻게 해야 하나요?

AMS Managed Active Directory 및 기타 공유 서비스 인프라 구성 요소는 AMS 운영자 액세스를 위해 설계되었습니다. Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹, AWS Organizations 서비스 제어 정책(SCP)을 업데이트하거나 이러한 구성 요소에 대한 전체 액세스를 유지하기 위해 다른 변경을 수행해야 할 수 있습니다.

Q: 오프보딩된 코어 계정을 해지할 수 있나요?

기본적으로 애플리케이션 계정에는 AWS Organizations 멤버십, 전송 게이트웨이 네트워크 연결, AMS Managed Active Directory를 통한 DNS 확인 등 MALZ Core 계정에 대한 여러 종속성이 있습니다. 이러한 종속성을 해결한 후 서비스 해제하고 오프보딩된 코어 계정을 해지할 수 있습니다. 자세한 내용은 [다중 계정 랜딩 존 계정](#) 단원을 참조하십시오.

코어 계정 오프보딩 RACI

- R: 책임 당사자. 나열된 작업을 완료할 책임이 있는 당사자입니다.
- A: 책임 당사자. 완료된 작업을 승인하는 당사자입니다.
- C: 상담 당사자. 일반적으로 주제 전문가로서 의견을 구하고 양자 통신이 이루어지는 당사자입니다.
- I: 정보 당사자. 종종 작업 또는 결과물 완료 시에만 진행 상황에 대한 정보를 받는 당사자입니다.

활동	Custom	AWS Managed Services(AMS)
사전 조건		
오프보딩할 각 AWS 계정 ID의 루트 이메일 주소에 대한 액세스 확인	R	C
관리 계정에 대한 액세스 확인 및 루트 사용자 전화번호 업데이트	R	C
권장 고객 작업에 대한 AMS 설명서 검토 및 AMS 오프보딩을 위한 계정 준비	R	C
오프보딩		
서비스 요청을 제출하여 랜딩 존 오프보딩 요청	R	정보

활동	Custome	AWS Managed Services(AMS)
코어 계정에서 AMS 구성 요소 오프보드	정보	R
오프보딩 후		
루트 사용자 계정 암호 재설정 및 오프보딩된 계정의 루트 액세스 확인	R	C
계정을 계속 운영하려면 AMS 오프보딩 설명서의 권장 고객 작업에 대한 AMS 지침을 따르거나 계정을 닫습니다.	R	C

오프보딩 변경 사항

다음 표에서는 AMS가 다중 계정 랜딩 존 오프보딩, 잠재적 영향 및 권장 작업에 대해 수행하는 작업을 설명합니다.

구성 요소	계정 유형	오프보딩을 위해 취한 조치	잠재적 영향	권장 고객 작업
액세스 관리	애플리케이션 계정	오프보딩 후 AMS 접속 호스트를 통해 EC2 스택에 액세스RFCs를 더 이상 제출할 수 없습니다. just-in-time	RFS를 통해 AMS 접속을 사용하여 EC2 인스턴스에 액세스할 수 없음	대체 방법을 사용하여 EC2 인스턴스에 액세스(참조 대체 액세스)
		AMS는 더 이상 기존 EC2 리소스 스택(PBIS Open 에이전트, 도메인 조인 스크립트)에서 액세스 관련 구성 요소를 관리하지 않습니다.	비 AMS 제공 AMIs에서 시작된 EC2 인스턴스가 Managed Active Directory 도메인에 조인되지 않음	기존 EC2 리소스 스택에서 AMS 시작 스크립트 제거(참조 AMS EC2 시작 스크립트 비활성화)
			제거하지 않으면 기존 리소스 스택의 AMS 시작 스크립트에서 AMS 종속성이 누락되어 오류가 발	

구성 요소	계정 유형	오프보딩을 위해 취한 조치	잠재적 영향	권장 고객 작업
			생하여 다른 도메인에 다시 가입하지 못할 수 있습니다.	
액세스 관리(계속)	코어 계정	PBIS Open에서 PBIS Enterprise(AD Bridge)로 마이그레이션한 경우 AMS는 코어 계정 오프보딩 후 더 이상 라이선스를 갱신하지 않습니다.	PBIS Enterprise 라이선스가 만료되도록 허용된 경우 Active Directory 자격 증명은 기존 Linux 기반 EC2 인스턴스 스택에 유효하지 않습니다.	PBIS Enterprise(AD Bridge)로 마이그레이션한 경우 라이선스 유지 또는 폐기 여부를 결정합니다(참조 PBIS Open/Enterprise(AD 브리지)).
로깅, 모니터링, 인시던트/이벤트 관리	애플리케이션 및 코어 계정	배포할 AMS 구성 요소가 제거 AMS의 기준 모니터링 알림됩니다. 기존에 배포된 Amazon CloudWatch 경보는 남아 있지만 더 이상 AMS 인시던트를 생성하지 않습니다. AWS Config AMS 및 MALZ Core 보안 계정의 집계 권한 부여가 제거됨 AWS Config 규칙은 배포된 상태로 유지되고 Amazon GuardDuty는 활성화된 상태로 유지되지만 더 이상 AMS 인시던트를 생성하지 않습니다.	새로 생성된 리소스에는 AMS 기준 모니터링 및 경보가 적용되지 않습니다. 인프라 지표 경보 및 보안 이벤트로 인해 더 이상 AMS 인시던트가 발생하지 않음 AWS Config 는 더 이상 중앙 계정에 집계되지 않습니다.	작업 지표를 정의, 캡처 및 분석하여 워크로드 이벤트를 보고 적절한 조치를 취합니다. 필요한 알림 워크플로를 구현하여 새 리소스에 필요한 운영 모니터링 및 경보를 계속 적용하고 AWS Config 및 Amazon GuardDuty에 구현합니다.

구성 요소	계정 유형	오프보딩을 위해 취한 조치	잠재적 영향	권장 고객 작업
연속성 관리(백업 및 복원)	애플리케이션 계정	AMS가 더 이상 백업 작업을 모니터링하거나 백업 및 복원 요청을 수행하지 않음 AMS 기본 백업 볼트, 백업 암호화 키 및 백업 역할이 남아 있음	백업 작업 실패가 발견되지 않을 수 있습니다.	백업 계획 구성 모니터링 및 검토
패치 관리	애플리케이션 및 코어 계정	AMS가 더 이상 성공적인 실행을 위해 패치 작업을 모니터링하거나 수동 패치 작업을 수행하지 않음 AMS가 더 이상 AMS 인프라 구성 요소를 업데이트하지 않음 AMS 제공 패치 기준은 유지됩니다. AMS 제공 AWS Systems Manager 패치 자동화 실행서는 공유되지 않으며 더 이상 사용할 수 없습니다.	패치 작업 실패가 발견되지 않을 수 있습니다. AMS 제공 Systems Manager Automation 런북에 의존하는 기존 패치 구성은 중단 없이 계속되도록 재구성해야 합니다.	필요에 따라 패치 구성 검토 및 재구성
네트워크 관리	애플리케이션 계정	지정된 경우 오프보딩된 애플리케이션 계정의 전송 게이트웨이 연결이 제거됩니다.	오프보딩된 애플리케이션 계정은 더 이상 전송 게이트웨이를 사용하여 Managed Active Directory 또는 기타 애플리케이션 계정과 같은 공유 서비스에 액세스할 수 없습니다.	전송 게이트웨이 연결을 유지False하려면 DeleteTransitGatewayAttachment로 지정

구성 요소	계정 유형	오프보딩을 위해 취한 조치	잠재적 영향	권장 고객 작업
보안 관리	애플리케이션 계정	계정이 중앙 Trend Micro 콘솔에서 분리됩니다. 또한 엔드포인트 에이전트는 더 이상 AMS 인시던트 프로세스를 통해 알림을 전달하지 않습니다. Trend Micro 에이전트는 설치된 상태로 유지되지만 AMS에서 더 이상 관리하거나 업데이트하지 않습니다. Trend Micro 에이전트를 배포하는 AMS 제공 AMI 사용자 지정은 더 이상 AMS에서 유지 관리하거나 업데이트하지 않습니다.	EC2 인스턴스 엔드포인트 맬웨어 탐지가 눈에 띄지 않을 수 있음 Trend 마이크로 에이전트는 AMS에서 제공하지 않는 AMI에서 시작된 EC2 인스턴스에 배포되지 않습니다. AMIs	Trend Micro를 계속하거나 중단하기 위한 옵션 고려(참조 Trend Micro Deep Security)
보안 관리(계속)	코어 계정	Trend Micro SQL 인프라는 공유 서비스 계정 내에 남아 있지만 AMS에서 더 이상 유지 관리하거나 업데이트하지 않습니다. Trend Micro"는 더 이상 AMS 인시던트 프로세스를 통해 알림을 전달하지 않습니다.	EC2 인스턴스 엔드포인트 맬웨어 탐지는 눈에 띄지 않을 수 있습니다. 인프라가 유지 관리되지 않는 경우(정의 업데이트, 라이선스 등) EC2 인스턴스 엔드포인트 보호가 영향을 받을 수 있습니다.	Trend Micro를 계속할지 또는 중단할지 결정(참조 Trend Micro Deep Security)

구성 요소	계정 유형	오프보딩을 위해 취한 조치	잠재적 영향	권장 고객 작업
변경 관리	애플리케이션 및 코어 계정	AMS RFC 콘솔 및 API가 제거됨 계정 수준 액세스 제한이 포함된 AMS 사용자 지정 서비스 제어 정책(SCPs)은 애플리케이션 계정 오프보딩 중에 분리되고 코어 계정 오프보딩 중에 삭제됩니다.	기본 AWS API를 사용하여 새 리소스를 생성하거나, 기존 리소스를 변경하거나, 기존 AWS CloudFormation 스택을 업데이트해야 합니다. AMS 제공 SCPs를 통해 계정 수준에서 액세스 제한이 더 이상 적용되지 않음	사용자 역할이 AWS 서비스를 사용하기에 충분한 액세스 권한을 제공하는지 확인합니다. SCP를 생성하여 계정 수준 권한 제한 제공
서비스 관리를 위한 AMS OS 이미지 및 자동화	애플리케이션 및 코어 계정	AMS는 더 이상 AMS 제공 EC2 AMIs AMS 제공 EC2 AMIs 오프보딩된 계정에서 계속 사용할 수 있습니다. AMS 제공 Systems Manager Automation 실행서는 공유되지 않으며 더 이상 사용할 수 없습니다.	오프보딩 후 AMS는 AMS 구성 요소에 대한 종속성이 누락FAILURE되어 cfn-signal AWS CloudFormation 전송으로 시작된 AMIs를 제공했습니다. AMS 제공 Systems Manager Automation 런북에 의존하는 운영 프로세스가 실패할 수 있습니다.	AMS 제공 AMIs 또는 Systems Manager Automation 런북에 의존하는 빌드 또는 운영 프로세스 검토 및 업데이트

구성 요소	계정 유형	오프보딩을 위해 취한 조치	잠재적 영향	권장 고객 작업
공유 서비스 인프라	코어 계정	AMS 액세스가 제거되고 AMS가 더 이상 AMS Managed Active Directory를 포함한 공유 구성 요소를 관리하지 않습니다 AWS Transit Gateway. AWS Organizations	공유 인프라에 대한 관리 손실	AMS Managed Active Directory에 대한 관리자 액세스 재설정 및 공유 서비스 구성 요소 관리 수임
보고	애플리케이션 및 코어 계정	AMS는 집계 보고를 위해 더 이상 계정 또는 리소스 수준 세부 정보를 수집하지 않습니다.	운영 및 비즈니스 지표(백업 및 패치 적용 범위, 변경 관리, 인시던트 활동)에 대한 인사이트 손실	계정 간 필요한 집계 데이터 보고를 자체 솔루션으로 대체
AMS 계정 팀 및 서비스 데스크	애플리케이션 및 코어 계정	AMS 계정 팀(CSDM, CA) 및 AMS 운영 서비스 데스크가 더 이상 오프보딩된 계정을 지원하지 않음	AMS에서 설계한 다중 계정 랜딩 존 아키텍처 및 관련 구성 요소에 대한 전문 지식으로 운영 지원 손실	환경에서 작업을 지원하기에 충분한 인력과 계정 구조 및 리소스에 대한 지식이 있는지 확인합니다.

대체 액세스

다음은 AMS 계정을 오프보딩한 후 EC2 스택에 대한 액세스를 유지하는 대체 방법입니다.

- 세션 관리자를 사용하면 접속이나 인바운드 네트워크 액세스 없이 권한이 상승된 EC2 인스턴스에 액세스할 수 있습니다. 자세한 내용은 [AWS Systems Manager Session Manager](#) 단원을 참조하십시오.
- 새 도메인 자격 증명을 사용하여 EC2 인스턴스를 다른 Active Directory 도메인에 다시 조인합니다. 를 사용하는 경우 디렉터리에 EC2 인스턴스 조인을 AWS Directory Service참조하세요. [EC2 AWS Managed Microsoft AD](#)
- 다른 액세스 방법 중 하나 또는 [AWS Systems Manager Run Command](#)를 통해 생성한 로컬 사용자 계정을 사용합니다.

AMS EC2 시작 스크립트 비활성화

Linux 운영 체제

배포의 패키지 관리자를 사용하여 `ams-modules` 패키지를 제거합니다. 예를 들어 Amazon Linux 2의 경우를 사용합니다 `yum remove ams-modules`.

Windows 운영 체제

Windows에서 EC2 시작 스크립트를 비활성화하려면 다음 단계를 완료하세요.

1. Windows Server 2008/2012/2012r2/2016/2019:

작업 스케줄러에서 관리형 서비스 시작 예약 작업을 비활성화하거나 제거합니다. 예약된 작업을 나열하려면 `Get-ScheduledTask -TaskName '*Ec2*'` 명령을 실행합니다.

Windows Server 2022:

[EC2Launch v2 작업을](#) 제거합니다. 이 작업은 인스턴스의 `C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml` Initialize-AMSBoot에서 `postReady` 단계에서 실행됩니다. 다음은 예제의 코드 조각입니다 `agent-config.yml`.

```
{
  "task": "executeScript",
  "inputs": [
    {
      "frequency": "always",
      "type": "powershell",
      "runAs": "localSystem"
    }
  ]
}
```

2. (선택 사항) 다음 파일 콘텐츠를 제거합니다.

```
C:\Program Files\WindowsPowerShell\Modules\AWSManagedServices.*
C:\Windows\System32\WindowsPowerShell\v1.0\Modules
\AWSManagedServices.Build.Utilities\*
```


PBIS Open/Enterprise(AD 브리지)

PBIS Open 또는 PBIS Enterprise(AD Bridge) 에디션을 사용하는지 확인하려면 Linux EC2 관리형 인스턴스에서 다음 명령을 실행합니다.

```
yum info | grep pbis
```

다음은 PBIS Enterprise(AD Bridge)를 보여주는 출력 예제입니다.

```
Name      : pbis-enterprise
From repo  : pbise
Name      : pbis-enterprise-devel
Repo      : pbise
Description : The pbis-enterprise-devel package includes the development
```

PBIS 열기

PBIS Open은 BeyondTrust가 더 이상 지원하지 않는 더 이상 사용되지 않는 제품입니다. 자세한 내용은 [BeyondTrust pbis-open 설명서를](#) 참조하세요.

AD 브리지(PBIS Enterprise)

다음 중 하나를 수행할 수 있습니다.

- 라이선스를 갱신하고 AD Bridge를 계속 운영합니다. 라이선싱 및 지원에 대해 알아보려면 BeyondTrust에 문의하세요.
- AD 브리지 사용을 중단합니다. 다음 Shell 명령을 실행하여 Linux 관리형 인스턴스에서 PBIS-Enterprise 패키지를 제거합니다. 자세한 내용은 BeyondTrust 설명서에서 [도메인 나가기 및 AD Bridge 에이전트 제거를 참조하세요](#).

```
$ sudo /opt/pbis/bin/uninstall.sh purge
```

PBIS 에이전트를 제거하지 않고 AMS 관리형 Active Directory 도메인을 그대로 둡니다.

PBIS 에이전트를 제거하지 않고 AMS 관리형 Active Directory를 나갈 수 있습니다. 운영 체제에 따라 다음 솔루션 중 하나를 사용합니다.

Linux operating systems

AMS 관리형 AD의 PBIS를 사용하여 다음 셸 명령을 실행하여 Linux EC2 인스턴스의 조인을 해제합니다. 자세한 내용은 사용하는 버전에 따라 [BeyondTrust pbis-open](#) 또는 [BeyondTrust AD Bridge](#) 설명서를 참조하세요.

```
$ sudo /opt/pbis/bin/domainjoin-cli leave
```

다음과 비슷한 오류 메시지가 표시될 수 있습니다.

```
Error: LW_ERROR_KRB5_REALM_CANT_RESOLVE [code 0x0000a3e1]  
Cannot resolve network address for KDC in requested realm
```

이 오류가 발생하면 다음 명령을 실행하여 AD 공급자 레지스트리를 삭제하고 lwsmd 서비스를 다시 시작합니다.

```
$ /opt/pbis/bin/regshell dir '[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers  
\ActiveDirectory\DomainJoin]'
```

이전 명령(예: **A123EXAMPLE.AMAZONAWS.COM**)에서 받은 디렉터리 ID 출력을 사용하여 다음 명령을 실행합니다.

```
$ /opt/pbis/bin/regshell delete_tree \  
'[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin  
\DIRECTORID]'  
  
$ /etc/pbis/redhat/lwsmd restart  
  
$ /opt/pbis/bin/lwsm restart lwreg
```

Windows operating systems

```
# Collect hostname and domain name using:  
  
Test-ComputerSecureChannel -verbose  
  
# Disjoin computer from the domain:  
  
netdom remove hostname /domain:domain name /force
```

Note

에 언급된 대로 관리형 서비스 시작 예약 작업을 비활성화하거나 제거해야 합니다. [AMS EC2 시작 스크립트 비활성화](#).

Trend Micro Deep Security

다음 옵션 중 하나를 사용하여 Trend Micro Deep Security 사용을 계속하거나 중단합니다.

계속 사용

- (전체 MALZ를 오프보딩하는 경우) 코어 계정 오프보딩 후 오프보딩된 애플리케이션 계정을 기존 Trend Micro Deep Security Manager(DSM)에 다시 연결하고 공유 서비스 계정의 라이선스를 유지합니다. 자세한 내용은 [AWS 클라우드 계정 추가 및 라이선스 정보 확인을 참조하세요](#).
- 1. 공유 서비스 계정에 로그인하고 Secrets Manager 콘솔로 이동합니다.
- 2. `/ams/eps/` 경로에 저장된 콘솔 관리자 자격 증명을 검색합니다.
- 3. <https://dsm.sentinel.int> 콘솔에 로그인합니다.
- 4. 교차 계정 역할 사용을 선택한 다음을 입력합니다 `arn:aws:iam::ACCOUNTID:role/mc_eps_cross_account_role`. ACCOUNTID를 오프보딩된 애플리케이션 계정 ID로 바꿉니다.
- 5. 다음을 선택합니다.
- 6. 몇 분 정도 기다렸다가 계정 검색을 처리하고 동기화가 성공했음을 표시합니다.
- 오프보딩된 애플리케이션 계정을 새 Trend Micro" 설치에 다시 연결합니다. 자세한 내용은 [에이전트 활성화 및 보호](#)와 [에이전트 활성화를 참조하세요](#).
- 오프보딩된 애플리케이션 계정을 Trend Micro Cloud One에 다시 연결합니다. 자세한 내용은 [Deep Security에서 워크로드 보안으로 마이그레이션](#) 및 [온프레미스에서 마이그레이션을 참조하세요](#).

사용 중단

- 오프보딩된 애플리케이션 계정에서 Trend Micro Deep Security Agents를 제거합니다. 자세한 내용은 [Deep Security 제거](#)를 참조하세요.

변경 관리 모드

AWS Managed Services(AMS)는 변경 관리 모드를 사용하여 AMS Advanced의 변경 사항을 보호합니다. 변경 관리 모드는 환경에 대한 높은 운영 표준을 유지하고 위험을 제어하고 부정적인 영향을 방지하는 데 도움이 됩니다. AMS Advanced에는 다양한 수준의 제어 및 위험을 제공하는 다양한 모드가 있습니다. 고객 관리형 모드를 제외한 모든 모드는 AMS에서 관리합니다. 사용 가능한 변경 관리 모드는 다음과 같습니다.

- RFC 모드(이전 표준 CM 모드): "변경 요청"(RFC) 시스템 및 AMS 사용자 지정 변경 유형(CTs)을 제공합니다.
- 직접 변경 모드: RFC 모드와 동일하며 AWS APIs 및 콘솔을 사용하여 AMS 관리형 리소스 생성
- AMS의 AWS Service Catalog: Direct Change 모드와 유사하지만 AMS 변경 관리 시스템(RFCs)을 사용하는 대신 AWS Service Catalog를 사용하여 AMS가 관리하는 리소스를 생성합니다.
- 개발자 모드: 직접 변경 모드와 동일 AWS APIs 및 콘솔을 사용하여 생성한 리소스만 AMS 관리형이 아니므로 사용자의 관리 책임은 사용자에게 있습니다.
- 셀프 서비스 프로비저닝(SSP) 모드: AMS 변경 관리 시스템에 액세스할 수 없다는 점을 제외하면 개발자 모드와 동일합니다(RFCs 없음).
- 고객 관리형 모드: AMS는 다중 계정 랜딩 존 랜딩 존을 제공하지만 모든 리소스 관리는 사용자의 책임입니다.

변경 관리(CM) API를 사용하는 AWS Managed Services(AMS) 변경 관리 시스템은 다중 계정 랜딩 존(MALZ) 및 단일 계정 랜딩 존(SALZ) 계정 모두에 대한 변경 요청(RFCs)을 생성하고 관리하는 작업을 제공합니다.

변경 요청(RFC)은 관리형 환경을 변경하기 위해 AMS 인터페이스를 통해 사용자 또는 AMS가 생성하는 요청이며 특정 작업에 대한 변경 유형(CT) ID를 포함합니다.

AMS 변경 관리(CM) API는 변경 요청(RFCs)을 생성하고 관리하는 작업을 제공합니다. RFCs. AMS 연산자는 RFCs으로 표시할 수 있습니다.

태그 또는 다른 이름에 사용할 수 없는 AMS 예약 접두사 목록은 [예약 접두사를 참조하세요](#).

스키마 및 예제를 포함하여 각 변경 유형에 대한 자세한 내용은 [AMS 변경 유형 참조](#)를 참조하세요.

Note

모든 변경 관리 API 호출은 AWS CloudTrail에 기록됩니다. 자세한 내용은 [로그 액세스를 참조하세요](#).

모드 개요

이 정보를 사용하면 비즈니스 성과를 달성하기 위해 원하는 유연성과 규범적 거버넌스 조합을 기반으로 애플리케이션을 호스팅하는 데 적합한 AWS Managed Services(AMS) 모드를 선택하는 데 도움이 됩니다.

이 정보의 대상은 다음과 같습니다.

- 랜딩 존의 전략 및 거버넌스를 담당하는 고객 팀. 이 정보는 팀이 내부 및 외부 고객에게 제공하려는 AMS 모드를 사용하여 AMS 관리형 랜딩 존의 기반을 마련하는 데 도움이 됩니다.
- 비즈니스 및 애플리케이션 소유자는 애플리케이션을 AMS로 마이그레이션하는 작업을 담당했습니다. 이 정보는 애플리케이션을 마이그레이션/호스팅하는 데 적합한 AMS 모드를 사용하여 애플리케이션 마이그레이션을 계획하는 데 도움이 됩니다. 참고로 소프트웨어 개발 수명 주기(SDLC) 수명 주기의 여러 단계에서 동일한 애플리케이션을 둘 이상의 AMS 모드에서 호스팅할 수 있습니다.
- AMS 파트너는 AMS를 구축하고 AMS로 마이그레이션하기 위한 다양한 옵션에 대해 고객을 안내하는 작업을 담당했습니다.

이 정보는 AMS 관리형 플랫폼 설정의 기초 단계와 AMS로의 온보딩이 완료되고 애플리케이션 거버넌스 및 운영에 집중한 직후 클라우드 채택 여정의 기초에서 마이그레이션 단계로 전환할 때 가장 유용합니다.

AMS의 모드 및 계정 유형

AWS Managed Services(AMS) 모드는 각 모드의 특정 거버넌스 프레임워크에 따라 AMS 서비스와 상호 작용하는 방법으로 정의할 수 있습니다. 랜딩 존 차이, 다중 계정 랜딩 존 또는 MALZ 및 단일 계정 랜딩 존 또는 SALZ가 기록됩니다.

Note

애플리케이션 배포 및 올바른 AMS 모드 선택에 대한 자세한 내용은 [AMS 모드 및 애플리케이션 또는 워크로드](#)를 참조하세요.

다양한 모드의 실제 사용 사례는 [AMS 모드의 실제 사용 사례를 참조하세요.](#)

다음 표에는 AMS 서비스당 모드에 대한 설명이 나와 있습니다.

AMS 기능	RFC 모드(이전 표준 CM 모드)/OOD*	직접 변경 모드	AWS Service Catalog	셀프 서비스 프로비저닝/개발자 모드	고객 관리형
랜딩 존 구성	MALZ 및 SALZ	MALZ 및 SALZ		MALZ 및 SALZ	
변경 관리	변경 일정, 수동 변경 사항 검토 및 변경 레코드	IAM 또는 보안 그룹과 같은 고위험 변경 사항에 대해 RFC 모드와 동일		없음	
로깅, 모니터링, 가드레일 및 이벤트 관리	예(지원되는 리소스)			아니요	
연속성 관리	예(지원되는 리소스)			해당 사항 없음/아니요	아니요
보안 관리	인스턴스 수준 보안 제어 및 계정 수준 제어			계정 수준 제어	AWS 조직 수준 제어
패치 관리	예			해당 사항 없음/아니요	아니요
인시던트 및 문제 관리	AMS 지원 리소스에 대한 응답 및 해결 SLA			결과 리소스에 대한 응답 SLA	아니요
보고	예			아니요	

AMS 기능	RFC 모드(이전 표준 CM 모드)/OOD*	직접 변경 모드	AWS Service Catalog	셀프 서비스 프로비저닝/개발자 모드	고객 관리형
서비스 요청 관리		예		지원 요청만	아니요

*OOD(Operations On Demand)에는 RFC 모드를 사용하는 고객이 전용 리소싱을 통해 변경 사항을 관리할 수 있는 기능이 있습니다. 자세한 내용은 [오퍼링의 온디맨드 운영 카탈로그](#)를 참조하고 클라우드 서비스 제공 관리자(CSDM)에게 문의하세요.

Note

[AMS의 셀프 서비스 프로비저닝 모드](#) 및는 모두 네이티브 AWS 서비스에 기반을 둔 복잡한 아키텍처가 있는 애플리케이션에 적합한 것으로 보일 [AMS 고급 개발자 모드](#) 수 있습니다. 워크로드를 설계할 때 비즈니스 컨텍스트에 따라 운영 우수성과 민첩성을 절충합니다. 이는 애플리케이션에 대해 SSP 모드 또는 개발자 모드를 선택할 때 고려할 수 있는 좋은 방법입니다. 선택 사항은 애플리케이션의 SDLC 단계에 따라 변경될 수도 있습니다. 예: 애플리케이션이 프로덕션 준비가 되면이 모드에서 AMS 가드레일이 더 엄격하기 때문에 SSP 모드가 더 적절한 옵션일 수 있습니다. 가드레일은 애플리케이션 OU 수준에서 IAM 업데이트 및 SCPs에 대한 RFC 기반 변경 제어와 같은 예방 제어 형태로 적용됩니다. 이러한 비즈니스 의사결정에 따라 엔지니어링 우선 순위가 달라질 수 있습니다. 거버넌스 및 운영 지원을 희생하면서 "pre-prod" 단계에서 애플리케이션 소유자의 유연성을 높이도록 최적화할 수 있습니다.

MALZ 아키텍처 및 관련 AMS 모드

AMS 다중 계정 랜딩 존(MALZ)은 기본 조직 단위(OU)인 고객 관리형 OU, 관리형 OU 또는 개발 OU에 따라 애플리케이션 계정(또는 리소스 계정)을 자동으로 프로비저닝할 수 있는 옵션을 제공합니다. 이러한 각 OUs로 생성된 애플리케이션 계정에 프로비저닝된 인프라에는 해당 기본 OUs에서 제공하는 특정 AMS 모드가 적용됩니다. 동일한 애플리케이션 계정에서 둘 이상의 모드를 혼합하여 찾는 것이 일반적입니다. 예를 들어 RFC 모드와 SSP 모드는 트리거 함수용 API Gateway 및 Lambda와 수집 및 오케스트레이션용 EC2, S3 및 SQS로 구성된 파이프라인 아키텍처를 호스팅하는 AMS 관리형 계정에 공존할 수 있습니다. 이 경우 SSP 모드가 Lambda 및 API Gateway에 적용됩니다.

그림 1은 AMS의 기본 OUs를 통해 다양한 모드가 제공되는 방법을 보여줍니다. AMS에서 새 애플리케이션 계정을 요청할 때는 계정의 OU를 선택해야 합니다.

MALZ 아키텍처 및 관련 AMS 모드

AMS는 서비스 제어 정책(SCPs)을 사용하여 계정을 논리적으로 관리하는 방법으로 AWS 모범 사례를 기반으로 하는 기본 OUs를 활용합니다. 이는 각 AMS 모드에서 거버넌스 프레임워크를 적용하는 방법입니다. 기본 OUs에 적용되는 모든 거버넌스 및 보안 가드레일(SCPs 형식)도 사용자 지정/하위 OUs에 자동으로 적용됩니다. 하위 OU에 대해 추가 SCPs를 요청할 수 있습니다. OUs 애플리케이션 계정이 모드와 동일하지 않다는 점을 이해하는 것이 중요합니다. 모드는 계정 내에 프로비저닝된 인프라에 적용되며 AMS와 고객 간의 운영 책임을 정의합니다.

그림 1: MALZ 아키텍처 및 관련 AMS 모드

Note

“제한적”이란 이러한 OUs에 대한 사용자 지정 정책을 요청할 수 있으며, 운영 우수성을 제공하는 AMS의 기능을 방해하지 않도록 case-by-case AMS의 승인을 받았음을 의미합니다. AMS 가드레일의 자세한 목록은 사용 설명서의 [AMS 가드레일을 참조하세요](#).

AMS 모드 및 애플리케이션 또는 워크로드

새 애플리케이션 계정을 요청하거나 기존 애플리케이션 계정에서 애플리케이션을 호스팅하여 올바른 모드를 선택할 때 애플리케이션의 운영 및 거버넌스 요구 사항을 고려합니다. 각 애플리케이션 또는 워크로드에 적합한 AMS 모드 선택은 다음 요인에 따라 달라집니다.

- 환경이 제공할 SDLC 수명 주기 함수의 유형(예: 변경 사항이 조정되지 않은 샌드박스, 자주 변경되는 UAT, 변경 사항이 최소화되고 규제가 엄격한 프로덕션)
- 필요한 거버넌스 정책(OU 수준에서 SCPs를 통해 적용됨)
- 운영 모델(운영 책임을 소유하거나 AMS에 아웃소싱하려는 경우)
- 클라우드 운영 시간, 운영 비용 등 원하는 비즈니스 성과.

Note

AMS 서비스당 모드 유형에 대한 설명은 [AMS의 모드 및 계정 유형을 참조하세요](#). 다양한 모드의 실제 사용 사례는 [AMS 모드의 실제 사용 사례를 참조하세요](#).

다음 표에는 애플리케이션 소유자가 가장 적합한 AMS 모드를 결정하는 데 도움이 되는 주요 고려 사항이 요약되어 있습니다. 애플리케이션 소유자는 특정 애플리케이션에 적용되는 모드를 완전히 이해하려면 애플리케이션 마이그레이션 전에 평가 단계를 포함해야 합니다. 예: 클라우드 네이티브 서비스 또는 서버리스 아키텍처 기반 애플리케이션의 경우 가장 좋은 옵션은 개발자 모드에서 빌드 및 반복을 시작하고 AMS 관리형 - SSP 모드를 사용하여 최종 코드형 인프라를 배포하는 것입니다. 이 경우 자동 배포를 위해 생성된 CloudFormation 템플릿이 AMS에서 제시한 수집 지침을 충족하는지 확인하기 위해 라이트 리팩터링이 필요할 수 있습니다. 또한 모든 IAM 권한은 최소 권한 모델을 따르도록 AMS Security의 승인을 받아야 합니다.

애플리케이션을 호스팅하도록 선택한 AMS 모드를 사용하면 원하는 클라우드 운영 모델을 구축할 수 있습니다.

Note

애플리케이션을 호스팅하기 위해 선택한 다양한 AMS 모드를 기반으로 단일 AMS 관리형 랜딩 존에 둘 이상의 클라우드 운영 모델이 존재할 수 있습니다.

결정 문제	표준 CM 모드/OD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형

운영 준비 상태

로깅, 모니터링 및 이벤트 관리	모든 관리형 인프라를 담당하는 AMS	셀프 서비스 프로비저닝 서비스 (SSP)를 담당하는 고객	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	고객 책임
연속성 관리	고객이 선택한 백업 계획을 실행할 AMS 책임	셀프 서비스 프로비저닝 서비스 (SSP)를 담당하는 고객	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프	

결정 문제	표준 CM 모드/ODD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
					로비저닝된 리소스를 담당하는 고객	
인스턴스 수준 액세스 관리	온프레미스 도메인과의 단방향 AD 신뢰를 통해 AMS 관리됩니다. 관리형 인프라가 AMS 도메인에 조인해야 함		해당 사항 없음		AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	
보안 관리 및 계정 수준 액세스 관리	모든 관리형 계정에 대한 AMS 책임		모든 관리형 계정을 담당하는 AMS		AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	
패치 관리	모든 관리형 계정에 대한 AMS 책임		셀프 서비스 프로비저닝 서비스 (SSP)를 담당하는 고객		AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
변경 관리	모든 관리형 계정에 대한 AMS 책임			셀프 서비스 프로비저닝 서비스 (SSP)를 담당하는 고객	AMS CM 시스템 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	
프로비저닝 관리	AMS에서 제공되는 프로비저닝 옵션에 대한 권장 및 표준화	AMS 규범적 표준에 따라 AWS Service Catalog용 AWS 서비스 API를 직접 사용할 수 있는 유연성	AMS 규범적 표준에 따라 AWS 서비스 API를 직접 사용할 수 있는 유연성	SSP 서비스에 AWS 서비스 APIs를 직접 사용할 수 있는 유연성	프로비저닝에 AWS 서비스 API를 직접 사용할 수 있는 유연성	
인시던트 관리 및 감사	모든 관리형 계정에 대한 AMS 책임				AMS Change Management System 외부에서 개발자 IAM 역할을 사용하여 프로비저닝된 리소스를 담당하는 고객	

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
GuardRails 및 공유 인프라(네트워크) 및 보안 프레임워크	AMS Core 계정의 권장 및 표준화 활용					유연한 맞춤형 AMS Core 계정 활용

애플리케이션 준비 상태

애플리케이션 리팩터링	라이트 리팩터링 필요	라이트 리팩터링 필요(AMS Standard CM을 사용하여 프로비저닝된 경우)	리팩터링 필요 없음
AWS 서비스 지원	AMS에서 지원하는 것으로 제한됨		제한되지 않음

비즈니스 고려 사항

운영 준비 시간	3~6개월	6개월 + 고객 애플리케이션 운영 역량에 따라 다름		고객 인프라 및 애플리케 이션 운영 역량에 따라 6~18개월
비용	\$\$\$\$	\$\$\$	\$\$	\$

결정 문제	표준 CM 모드/OOD*	AWS Service Catalog	직접 변경 모드	셀프 서비스 프로비저닝	개발자 모드	고객 관리형
애플리케이션 예제	3 티어 스택이 있는 Webserver, 규정 준수 및 규제 요구 사항이 있는 앱			API Gateway를 사용하는 Webserver, ECS/EKS를 활용하는 컨테이너화된 애플리케이션	Lambda, Glue, Athena 등을 사용하는 Data Lake 애플리케이션에서 반복/최적화	샌드박스, 타사 관리형 애플리케이션과 같은 분산형 계정/애플리케이션

*OOD(Operations On Demand)에는 표준 CM 모드를 사용하는 고객이 전용 리소싱을 통해 변경 사항을 관리할 수 있는 기능이 있습니다. 자세한 내용은 [오퍼링의 온디맨드 운영 카탈로그](#)를 참조하고 클라우드 서비스 제공 관리자(CSDM)에게 문의하세요.

Note

SSP 모드와 개발자 모드 간의 가격 비교는 동일한 AWS 서비스가 프로비저닝된다고 가정합니다.

AMS 모드와 비즈니스 및 IT 목표 비교

그림과 같이 애플리케이션에 대해 고도로 제어되고 표준화된 거버넌스 모델을 찾고 있다면 AMS 관리형 표준 변경, AWS Service Catalog 또는 직접 변경 모드가 가장 적합합니다. 운영 준비 없이 애플리케이션 혁신에 중점을 둔 맞춤형 거버넌스 모델이 필요한 경우 고객 관리형 모드를 선택합니다. 고객 관리형 모드를 사용하면 인시던트 관리, 구성 관리, 프로비저닝 관리, 보안 관리, 패치 관리 등과 같은 운영 기능을 지원하는 인력, 프로세스 및 도구를 구축할 책임이 있으므로 애플리케이션을 운영하는 데 시간이 더 오래 걸릴 수 있습니다.

AMS 모드의 실제 사용 사례

이를 검토하여 AMS 모드를 사용하는 방법을 결정합니다.

- 사용 사례 1, 시간에 민감한 데이터 센터 종료와 함께 비용을 절감하기 위한 비즈니스 요구 사항: 데이터 센터 종료와 같은 매력적인 비즈니스 이벤트가 있는 기업은 클라우드에서 온프레미스 애플리케이션을 다시 호스팅하는 데 관심이 있습니다. 대부분의 온프레미스 인벤토리는 운영 체제 버전이 혼합된 Windows 및 Linux 서버로 구성됩니다. 이를 통해 고객은 클라우드로 전환하여 애플리케이션의 기술 및 보안 태세를 개선하는 비용 절감을 활용하고자 합니다. 고객은 빠르게 움직이고 싶지만 아직 사내 클라우드 운영 전문 지식이 구축되어 있지 않습니다. 고객은 리팩터링의 균형을 찾아야 합니다. 리팩터링이 너무 많으면 촉박한 타임라인에 비해 위험할 수 있습니다. 그러나 OS 버전 업데이트 및 데이터베이스 최적화와 같은 일부 리팩터링을 통해 애플리케이션은 다음 수준의 성능을 달성할 수 있습니다. 이 예제에서 고객은 AMS 관리형 RFC 모드를 선택하여 대부분의 애플리케이션을 다시 호스팅할 수 있습니다. AMS는 인프라 운영을 제공하는 동시에 고객 운영 팀에 클라우드에서 안전하게 운영하는 모범 사례를 안내합니다.

AMS 관리형 AWS Service Catalog 및 AMS 관리형 Direct Change 모드는 고객에게 동일한 비즈니스 성과와 목표를 달성하면서 유연성을 높입니다. 또한 고객은 AMS Operations On Demand(OOD) 오퍼링을 사용하여 전용 AMS 운영 엔지니어가 변경 요청(RFCs).

차별화되지 않은 인프라 운영 작업(패치, 백업, 계정 관리 등)을 AMS로 오프로드하는 동안 고객은 애플리케이션을 최적화하는 데 계속 집중하고 클라우드 운영에서 내부 팀을 확장할 수 있습니다. AMS는 고객에게 비용 절감에 대한 월별 보고서를 제공하고 리소스 최적화에 대한 권장 사항을 제시합니다. 이 사용 사례에서는 Windows 2003 및 2008과 같은 레거시 OS 버전에서 호스팅된 end-of-life 애플리케이션이 있고 고객이 리팩터링하지 않기로 결정한 경우 해당 애플리케이션을 AMS로 마이그레이션하고 고객 관리형 모드를 활용하는 계정에서 호스팅할 수도 있습니다.

- 사용 사례 2, 보안 AMS 경계 내에서 Lambda, Glue, Athena로 데이터 레이크 구축: 기업은 AMS의 여러 애플리케이션에 대한 보고 요구 사항을 충족하기 위해 Data Lake를 설정하려고 합니다. 고객은 S3 버킷을 사용하여 데이터 세트를 저장하고 AWS Athena를 사용하여 각 보고서의 데이터 세트를 쿼리하려고 합니다. S3와 AWS Athena는 별도의 AMS 관리형 계정에 배포됩니다. S3가 있는 계정에는 데이터 수집 파이프라인을 빌드하기 위한 Glue, Lambda 및 Step Functions와 같은 다른 서비스도 있습니다. 이 경우 Glue, Lambda, Athena 및 Step Functions는 셀프 서비스 프로비저닝(SSP) 서비스로 간주됩니다. 또한 고객은 임시 도구/스크립팅 서버 역할을 하는 계정에 EC2 인스턴스를 배포했습니다. 고객은 먼저 AMS 관리형 계정에서 SSP 서비스를 활성화하도록 AMS에 요청합니다. AMS는 역할이 고객의 연동 솔루션에 온보딩되면 고객이 수임할 수 있는 각 서비스에 대해 IAM 역할을 프로비저닝합니다. 간편한 관리를 위해 고객은 별도의 IAM 역할에 대한 정책을 하나의 사용자 지정 역할로 결합하여 AWS 서비스 간에 작업할 때 역할을 전환할 필요성을 줄일 수도 있습니다. 계정에서 역할이 활성화되면 고객은 요구 사항에 따라 서비스를 구성할 수 있습니다. 그러나 고객은 AMS 변경 관리 시스템과 협력하여 사용 사례에 따라 추가 권한을 요청해야 합니다.

예를 들어 Glue 크롤러에 액세스하려면 Glue에 추가 권한이 필요합니다. Lambda에 대한 이벤트 소스를 생성하려면 추가 권한도 필요합니다. 고객은 AMS와 협력하여 Athena가 S3 버킷을 쿼리할 수 있도록 교차 계정 액세스를 허용하도록 IAM 역할을 업데이트합니다. Lambda가 Step Functions 서비스를 호출하고 Glue가 모든 S3 버킷을 읽고 쓸 수 있도록 AMS 변경 관리를 통해 서비스 역할 또는 서비스 연결 역할을 업데이트해야 합니다. AMS는 고객과 협력하여 최소 권한 액세스 모델을 따르고 요청된 IAM 변경 사항이 지나치게 허용적이지 않고 불필요한 위험에 노출되지 않도록 합니다. 고객의 데이터 레이크 팀은 고객의 아키텍처와 관련된 서비스에 필요한 모든 IAM 권한을 계획하고 AMS에 이를 활성화하도록 요청합니다. 이는 모든 IAM 변경 사항이 수동으로 처리되고 AMS 보안 팀의 검토를 받기 때문입니다. 이러한 요청을 처리하는 데 걸리는 시간은 애플리케이션 배포 일정에서 고려해야 합니다.

SSP 서비스가 계정에서 작동하므로 고객은 AMS 인시던트 관리 및 서비스 요청을 통해 지원을 요청하고 문제를 보고할 수 있습니다. 그러나 AMS는 Lambda에 대한 성능 및 동시성 지표 또는 Glue에 대한 작업 지표를 적극적으로 모니터링하지 않습니다. SSP 서비스에 대해 적절한 로깅 및 모니터링이 활성화되었는지 확인하는 것은 고객의 책임입니다. 계정의 EC2 인스턴스 및 S3 버킷은 AMS에서 완전히 관리됩니다.

- 사용 사례 3, AMS에서 CICD 배포 파이프라인의 빠르고 유연한 설정: 고객이 AMS의 모든 애플리케이션 계정에 코드 파이프라인을 배포하기 위해 Jenkins 기반 CICD 파이프라인을 설정하려고 합니다. 고객은 AMS 관리형 Direct Change 모드(DCM) 또는 AMS 관리형 개발자 모드에서이 CICD 파이프라인을 호스팅하는 것이 가장 적합할 수 있습니다. 이는 아티팩트 리포지토리를 호스팅하는 CloudFormation 및 S3 버킷에 액세스할 수 있는 원하는 IAM 권한과 함께 EC2에 필요한 사용자 지정 구성으로 Jenkins 서버를 유연하게 설정할 수 있기 때문입니다. AMS 관리형 RFC 모드에서도이 작업을 수행할 수 있지만 고객 팀은 IAM 역할에 대해 여러 개의 수동 RFCs를 생성하여 AMS에서 수동으로 검토하는 최소 허용 권한 세트를 반복해야 합니다. DCM을 사용하면 AMS 관리형 RFCs 대한 수동 RFC를 여러 개 생성할 필요 없이 AWS에서 운영 목표를 달성하여 AMS에서 수동으로 검토하는 최소 허용 권한 세트를 반복할 수 있습니다. AMS 프로세스와 도구를 늘리려면 고객 측 교육뿐만 아니라 시간이 걸립니다. 개발자 모드에서 고객은 "개발자 역할"로 시작하여 네이티브 AWS APIs. 이 파이프라인을 설정하는 가장 빠르고 유연한 방법은 AMS Managed-Developer 모드를 사용하는 것입니다. 개발자 모드는 운영 통합을 손상시키면서 가장 빠르고 쉬운 방법을 제공하는 반면, DCM은 덜 유연하지만 RFC 모드와 동일한 수준의 운영 지원을 제공합니다.
- 사용 사례 4, AMS 기반 내의 맞춤형 운영 모델: 고객이 기한 기반 데이터 센터 종료를 보고 있으며, 애플리케이션 운영 및 인프라 운영을 포함한 타사 MSP가 엔터프라이즈 애플리케이션 중 하나를 완전히 관리합니다. AMS에서 운영할 수 있도록 고객이 일정애이 애플리케이션을 리팩터링할 시간이 없다고 가정하면 고객 관리형 모드가 적절한 옵션입니다. 고객은 AMS 관리형 랜딩 존의 자동 및 빠른 설정을 활용할 수 있습니다. 중앙 집중식 네트워킹 계정을 통해 계정 벤딩 및 연결을 제어하는 중앙 집중식 계정 관리를 활용할 수 있습니다. 또한 AMS Payer 계정을 통해 모든 고객 관리형 계정에

대한 요금을 통합하여 결제를 간소화합니다. 고객은 AMS 관리형 계정에 사용되는 표준 액세스 관리와 별도로 MSP를 사용하여 맞춤형 액세스 관리 모델을 유연하게 설정할 수 있습니다. 이렇게 하면 고객 관리형 모드를 사용하여 온프레미스 환경을 비우는 비즈니스 요구 사항을 충족하면서 AMS 관리형 환경을 설정할 수 있습니다. 이 경우 고객이 클라우드로 마이그레이션하는 Windows 기반 애플리케이션도 보유하고 있고 이를 고객 관리형 계정으로 이동하기로 선택한 경우 고객은 클라우드 운영 모델을 생성할 책임이 있습니다. 이는 기존 IT 프로세스를 혁신하고 인력을 교육하는 고객의 능력에 따라 복잡하고 비용이 많이 들고 시간이 많이 걸릴 수 있습니다. 고객은 이러한 워크로드를 AMS 관리형 계정으로 "리프트 앤 시프트"하여 시간과 비용을 절약하고 인프라 작업을 AMS로 오프로드할 수 있습니다.

Note

고객은 RFC 또는 SSP 모드의 거버넌스 프레임워크와 개발자 모드 간에 애플리케이션 계정을 이동해야 할 때가 있습니다. 예를 들어 고객은 초기 리프트 앤 시프트 마이그레이션의 일부로 AMS 관리형 모드에서 애플리케이션을 호스팅할 수 있지만, 초과 근무 시 애플리케이션을 다시 작성하여 클라우드 네이티브 AWS 서비스에 최적화하려고 합니다. 사전 프로덕션 계정의 모드를 AMS 관리형 RFC에서 AMS 관리형 개발자 모드로 변경하여 인프라를 프로비저닝할 수 있는 유연성과 민첩성을 제공할 수 있습니다. 그러나 "개발자 역할"을 사용하여 인프라 프로비저닝을 변경한 후에는 동일한 인프라를 AMS 관리형 RFC 모드로 다시 이동할 수 없습니다. 이는 AMS가 AMS 변경 관리 시스템 외부에서 프로비저닝된 인프라의 운영을 보장할 수 없기 때문입니다. 고객은 AMS 관리형 RFC 모드를 제공하는 새 애플리케이션 계정을 생성한 다음 AMS 관리형 계정으로 수집된 CloudFormation 템플릿 또는 사용자 지정 AMIs를 통해 "최적화된" 인프라 구성을 다시 배포해야 할 수 있습니다. 이는 프로덕션 준비 구성을 배포하는 깔끔한 방법입니다. 배포되면 애플리케이션은 규범적 AMS 거버넌스 및 운영의 적용을 받습니다. 고객 관리형 모드와 AMS 관리형 모드 간 전환 모드에도 동일하게 적용됩니다.

RFC 모드

RFC 모드는 AMS Advanced 운영 계획 고객의 기본 모드입니다. 여기에는 변경 또는 RFCs에 대한 요청이 있는 변경 관리 시스템과 계정에 필요한 추가 또는 변경을 요청하는 데 사용할 변경 유형 카탈로그가 포함됩니다. 이 변경 관리 시스템은 계정을 변경할 수 있는 사용자를 제한하는 데 있어 보안 수준을 제공합니다.

AMS 고급 변경 유형에 대한 자세한 내용은 [AMS 변경 유형이란 무엇입니까?](#)를 참조하세요.

AMS Advanced 온보딩에 대한 자세한 내용은 [AWS Managed Services 온보딩 소개](#)를 참조하세요.

변경 유형 예제 연습은 AMS 고급 변경 유형 참조 분류별 변경 유형 [섹션의 관련 변경 유형에 대한 "추가 정보" 섹션을 참조하세요.](#)

 Note

RFC 모드는 이전에 "변경 관리 모드" 또는 "표준 CM 모드"라고 불렸습니다.

주제

- [RFCs 대해 알아보기](#)
- [변경 유형이란 무엇입니까?](#)
- [AMS의 RFC 오류 문제 해결](#)

RFCs 대해 알아보기

변경 요청 또는 RFCs는 두 가지 방식으로 작동합니다. 먼저 RFC 자체에 필요한 파라미터가 있습니다. API의 옵션은 다음과 같습니다CreateRfc. 둘째, RFC의 작업에 필요한 파라미터(실행 파라미터)가 있습니다. CreateRfc 옵션에 대해 알아보려면 AMS API 참조의 [CreateRfc](#) 섹션을 참조하세요. 이러한 옵션은 일반적으로 RFC 생성 페이지의 추가 구성 영역에 나타납니다.

CreateRfc API, `aws amscm create-rfc` CLI 또는 AMS 콘솔 RFC 생성 페이지를 사용하여 RFC를 생성하고 제출할 수 있습니다. RFC 생성에 대한 자습서는 섹션을 참조하세요[RFC 생성](#).

주제

- [RFCs란 무엇입니까?](#)
- [AMS API/CLI 사용 시 인증](#)
- [RFC 보안 검토 이해](#)
- [RFC 변경 유형 분류 이해](#)
- [RFC 작업 및 활동 상태 이해](#)
- [RFC 상태 코드 이해](#)
- [RFC 업데이트 CTs 및 CloudFormation 템플릿 드리프트 감지 이해](#)
- [RFCs 예약](#)
- [RFCs 승인 또는 거부](#)
- [RFC 제한 실행 기간 요청](#)

- [RFCs 생성, 복제, 업데이트, 찾기 및 취소](#)
- [RFCs와 함께 AMS 콘솔 사용](#)
- [일반적인 RFC 파라미터에 대해 알아보기](#)
- [RFC 일일 이메일에 가입](#)

RFCs란 무엇입니까?

변경 요청 또는 RFC는 AMS 관리형 환경을 변경하거나 AMS에 사용자를 대신하여 변경하도록 요청하는 방법입니다. RFC를 생성하려면 AMS 변경 유형 중에서 선택하고 RFC 파라미터(예: 일정)를 선택한 다음 AMS 콘솔 또는 API 명령 [CreateRfc](#) 및 [SubmitRfc](#)를 사용하여 요청을 제출합니다.

RFC에는 두 가지 사양이 있습니다. 하나는 RFC 자체용이고 다른 하나는 변경 유형(CT) 파라미터용입니다. 명령줄에서 인라인 RFC 명령 또는 JSON 형식의 표준 CreateRfc 템플릿을 사용하여 생성한 CT JSON 스키마 파일(CT 파라미터 기반)과 함께 작성하고 제출할 수 있습니다. CT 이름은 CT에 대한 비공식 설명입니다. CSIO(범주, 하위 범주, 항목, 작업)는 CT에 대한 보다 공식적인 설명입니다. RFC를 생성할 때 CT ID만 지정해야 합니다.

AMS는 변경이 성공적으로 완료되거나(성공) 실패하면(실패) 알려줍니다.

Note

RFC 실패 문제 해결에 대한 자세한 내용은 섹션을 참조하세요 [AMS의 RFC 오류 문제 해결](#).

다음 그림은 사용자가 제출한 RFC의 워크플로를 보여줍니다.

AMS API/CLI 사용 시 인증

AMS API/CLI를 사용하는 경우 임시 자격 증명으로 인증해야 합니다. 페더레이션 사용자를 위한 임시 보안 자격 증명을 요청하려면 [GetFederationToken](#), [AssumeRole](#), [AssumeRoleWithSAML](#) 또는 [AssumeRoleWithWebIdentity](#) AWS 보안 토큰 서비스(STS) APIs.

일반적인 선택은 SAML입니다. 설정 후 호출하는 각 작업에 인수를 추가합니다. 예를 들어 `aws --profile sam1 amscm list-change-type-categories`입니다.

SAML 2.0 프로파일의 바로 가기를 사용하여 각 API/CLI 시작 시 프로파일 변수를 설정하는 것입니다 `set AWS_DEFAULT_PROFILE=sam1`(Windows의 경우, Linux의 경우 `export`

AWS_DEFAULT_PROFILE=saml). CLI 환경 변수 설정에 대한 자세한 내용은 [AWS 명령줄 인터페이스 구성, 환경 변수를 참조하세요](#).

RFC 보안 검토 이해

AWS Managed Services(AMS) 변경 관리 승인 프로세스를 통해 계정의 변경 사항에 대한 보안 검토를 수행할 수 있습니다.

AMS는 AMS 기술 표준을 기준으로 모든 변경 요청(RFCs) 평가합니다. 기술 표준을 벗어나 계정의 보안 태세를 저하시킬 수 있는 모든 변경 사항은 보안 검토를 거칩니다. 보안 검토 중에 AMS는 관련 위험을 강조 표시하고, 보안 위험이 높거나 매우 높은 경우 승인된 보안 담당자가 RFC를 수락하거나 거부합니다. 또한 모든 변경 사항을 평가하여 AMS의 운영 능력에 부정적인 영향을 미치는지 평가합니다. 잠재적인 부정적인 영향이 발견되면 AMS 내에서 추가 검토 및 승인이 필요합니다.

AMS 기술 표준

AMS 기술 표준은 최소 보안 기준, 구성 및 프로세스를 정의하여 계정의 기본 보안을 설정합니다. AMS와 사용자 모두 이러한 표준을 따라야 합니다.

기술 표준을 벗어나 계정의 보안 태세를 잠재적으로 저하시킬 수 있는 모든 변경 사항은 위험 수락 프로세스를 거칩니다. 이 프로세스에서는 AMS에서 관련 위험을 강조 표시하고 권한 있는 보안 담당자가 사용자 측에서 수락하거나 거부합니다. 또한 이러한 모든 변경 사항을 평가하여 AMS의 계정 운영 능력에 부정적인 영향을 미칠지 여부를 평가하고, 영향을 미칠 경우 AMS 내에서 추가 검토 및 승인이 필요한지 여부를 평가합니다.

RFC 고객 보안 위험 관리(CSRM) 프로세스

조직의 누군가가 관리형 환경에 대한 변경을 요청하면 AMS는 변경 사항을 검토하여 해당 요청이 기술 표준을 벗어나 계정의 보안 태세를 저하시킬 수 있는지 확인합니다. 요청이 계정의 보안 태세를 저하시키는 경우 AMS는 보안 팀에 관련 위험을 알리고 변경을 실행합니다. 또는 변경으로 인해 환경에서 보안 위험이 높거나 매우 높은 경우 AMS는 위험 수락(다음 설명됨)의 형태로 보안 팀 연락처로부터 명시적 승인을 구합니다. AMS 고객 위험 수락 프로세스는 다음을 위해 설계되었습니다.

- 위험을 명확하게 식별하고 올바른 소유자에게 알립니다.
- 환경에 대해 식별된 위험 최소화
- 조직의 위험 프로필을 이해하는 지정된 보안 담당자로부터 승인을 받고 문서화합니다.
- 식별된 위험에 대한 지속적인 운영 오버헤드 감소

기술 표준 및 높거나 매우 높은 위험에 액세스하는 방법

<https://console.aws.amazon.com/artifact/> AMS 기술 표준 설명서를 보고서로 참조할 수 있도록 했습니다. AMS 기술 표준 설명서를 사용하여 변경 요청(RFC)을 제출하기 전에 승인된 보안 담당자의 위험 수락이 변경에 필요한지 여부를 파악합니다.

기본 AWSManagedServicesChangeManagementRole로 로그인한 후 보고서 탭 검색 창에서 "AWS Managed Services(AMS) 기술 표준" AWS Artifact 을 검색하여 기술 표준 보고서를 찾습니다.

Note

AMS 기술 표준 문서는 단일 계정 랜딩 존의 Customer_ReadOnly_Role에 액세스할 수 있습니다. 다중 계정 랜딩 존에서는 보안 관리자가 사용하는 AWSManagedServicesAdminRole과 애플리케이션 팀이 사용하는 AWSManagedServicesChangeManagementRole을 사용하여 문서에 액세스할 수 있습니다. 팀에서 사용자 지정 역할을 사용하는 경우 기타 | 기타 RFC를 생성하여 액세스를 요청하면 지정된 사용자 지정 역할이 업데이트됩니다.

RFC 변경 유형 분류 이해

RFC를 제출할 때 사용하는 변경 유형은 두 가지 광범위한 범주로 나뉩니다.

- 배포: 이 분류는 리소스를 생성하기 위한 것입니다.
- 관리: 이 분류는 리소스를 업데이트하거나 삭제하기 위한 것입니다. 관리 범주에는 인스턴스 액세스, AMIs 암호화 또는 공유, 스택 시작, 중지, 재부팅 또는 삭제를 위한 변경 유형도 포함됩니다.

RFC 작업 및 활동 상태 이해

RfcActionState (API) / 활동 상태(콘솔)는 RFC에서 사람의 개입 또는 작업 상태를 이해하는 데 도움이 됩니다. 주로 수동 RFCs에 사용되는 RfcActionState는 사용자 또는 AMS 작업에 필요한 작업이 있는 시기를 이해하고 AMS 작업이 RFC에서 활발하게 작업하는 시기를 확인하는 데 도움이 됩니다. 이렇게 하면 수명 주기 동안 RFC에서 수행되는 작업에 대한 투명성이 향상됩니다.

RfcActionState (API) / 활동 상태(콘솔) 정의:

- AwsOperatorAssigned: AWS 운영자가 RFC에서 적극적으로 작업하고 있습니다.
- AwsActionPending: AWS의 응답 또는 작업이 예상됩니다.
- CustomerActionPending: 고객의 응답 또는 조치가 필요합니다.

- NoActionPending: AWS 또는 고객의 조치가 필요하지 않습니다.
- NotApplicable: 이 상태는 AWS 운영자 또는 고객이 설정할 수 없으며 기능이 릴리스되기 전에 생성된 RFCs에만 사용됩니다.

RFC 작업 상태는 제출된 변경 유형에 수동 검토가 필요한지 여부와 일정이 ASAP로 설정되어 있는지 여부에 따라 달라집니다.

- 지연된 일정으로 수동 변경 유형을 검토, 승인 및 시작하는 동안 RFC ActionState가 변경됩니다.
- 예약된 수동 RFC를 제출하면 ActionState가 자동으로 AwsActionPending으로 변경되어 운영자가 RFC를 검토하고 승인해야 함을 나타냅니다.
- 운영자가 RFC를 적극적으로 검토하기 시작하면 ActionState가 AwsOperatorAssigned로 변경됩니다.
- 운영자가 RFC를 승인하면 RFC 상태가 예약됨으로 변경되고 ActionState가 자동으로 NoActionPending으로 변경됩니다.
- RFC의 예약된 시작 시간에 도달하면 RFC 상태가 InProgress으로 변경되고 ActionState가 자동으로 AwsActionPending으로 변경되어 RFC 검토를 위해 연산자를 할당해야 함을 나타냅니다.
- 운영자가 RFC를 적극적으로 실행하기 시작하면 ActionState를 AwsOperatorAssigned로 변경합니다.
- 완료되면 연산자가 RFC를 닫습니다. 그러면 ActionState가 NoActionPending으로 자동 변경됩니다.

Important

- 작업 상태는 사용자가 설정할 수 없습니다. RFC의 변경 사항에 따라 자동으로 설정되거나 AMS 연산자가 수동으로 설정합니다.
- RFC에 대응 서신을 추가하면 ActionState가 자동으로 AwsActionPending으로 설정됩니다.
- RFC가 생성되면 ActionState가 자동으로 NoActionPending으로 설정됩니다.
- RFC가 제출되면 ActionState는 자동으로 AwsActionPending으로 설정됩니다.
- RFC가 거부됨, 취소됨 또는 성공 또는 실패 상태로 완료되면 ActionState가 자동으로 NoActionPending으로 재설정됩니다.
- 작업 상태는 자동 RFCs 모두에 대해 활성화되지만, 대부분 수동 RFCs의 경우 이러한 유형의 RFCs에 통신이 필요한 경우가 많기 때문에 중요합니다.

RFC 작업 상태 사용 사례 검토

사용 사례: 수동 RFC 프로세스에 대한 가시성

- 수동 RFC를 제출하면 운영자가 RFC를 검토하고 승인해야 함을 나타내 `AwsActionPending` 기 위해 RFC 작업 상태가 `로` 자동 변경됩니다. 운영자가 RFC를 적극적으로 검토하기 시작하면 RFC 작업 상태가 `로` 변경됩니다 `AwsOperatorAssigned`.
- 승인 및 예약되어 실행을 시작할 준비가 된 수동 RFC를 생각해 보세요. RFC 상태가 `로` 변경되면 `InProgress` RFC 작업 상태가 자동으로 `로` 변경됩니다 `AwsActionPending`. 운영자가 RFC를 적극적으로 실행하기 시작 `AwsOperatorAssigned` 하면 다시 `로` 변경됩니다.
- 수동 RFC가 완료되면("성공" 또는 "실패"로 닫힘) RFC 작업 상태가 `로` 변경 `NoActionPending` 되어 고객 또는 운영자의 추가 작업이 필요하지 않음을 나타냅니다.

사용 사례: RFC 대응

- 수동 RFC가 인 경우 AMS 운영자 `Pending Approval` 가 추가 정보를 필요로 할 수 있습니다. 연산자는 RFC에 서신을 게시하고 RFC 작업 상태를 `로` 변경합니다 `CustomerActionPending`. 새 RFC 대응 서신을 추가하여 응답하면 RFC 작업 상태가 자동으로 `로` 변경됩니다 `AwsActionPending`.
- 자동 또는 수동 RFC가 실패하면 RFC 세부 정보에 서신을 추가하여 AMS 운영자에게 RFC가 실패한 이유를 물어볼 수 있습니다. 서신이 추가되면 RFC 작업 상태가 자동으로 `로` 설정됩니다 `AwsActionPending`. AMS 운영자가 서신을 보기 위해 RFC를 선택하면 RFC 작업 상태가 `로` 변경됩니다 `AwsOperatorAssigned`. 연산자가 새 RFC 대응 서신을 추가하여 응답할 때 RFC 작업 상태를 `로` 설정하여 고객의 다른 응답이 있음을 `CustomerActionPending` 나타내거나 `NoActionPending`로 설정하여 고객의 응답이 필요하지 않거나 예상되지 않음을 나타낼 수 있습니다.

RFC 상태 코드 이해

RFC 상태 코드는 요청을 추적하는 데 도움이 됩니다. CLI 출력에서 RFC를 실행하는 동안 또는 콘솔에서 RFC 목록 페이지를 새로 고쳐 이러한 상태 코드를 관찰할 수 있습니다.

해당 RFC의 세부 정보 페이지에서 다음과 같은 RFC의 코드를 볼 수도 있습니다.

목록에 제출하지 않은 RFC가 표시될 수 있습니다. AMS 연산자가 내부 전용 CT를 사용하는 경우 RFC에 제출하고 RFC 목록에 표시됩니다. 자세한 내용은 [내부 전용 변경 유형](#) 단원을 참조하십시오.

⚠ Important

RFC 상태 변경에 대한 알림을 요청할 수 있습니다. 자세한 내용은 [RFC 상태 변경 알림을 참조하세요](#).

RFC 상태 코드

Success	실패
편집: RFC가 생성되었지만 제출되지 않음 PendingApproval / Submitted: RFC가 제출되었으며 시스템에서 승인이 필요한지 여부를 결정하고 필요한 경우 해당 승인을 얻고 있습니다. AWS에서 승인/고객이 승인: RFC가 승인되었습니다. 자동 RFCs는 AWS의 승인을 받고 수동 RFCs는 운영자 및 경우에 따라 고객의 승인을 받습니다. 예약됨: RFC가 구문 및 요구 사항 검사를 통과했으며 실행이 예약됨 InProgress: RFC가 실행 중입니다. 여러 리소스를 프로비저닝하거나 오래 실행되는 UserData가 있는 RFCs는 실행하는 데 시간이 더 오래 걸립니다. 실행됨: RFC가 실행되었습니다. 성공/성공: RFC가 성공적으로 완료되었습니다.	거부됨: RFCs는 일반적으로 검증에 실패하기 때문에 거부됩니다. 예를 들어 사용할 수 없는 리소스, 즉 서브넷이 지정됩니다. 취소됨: RFCs는 일반적으로 구성된 시작 시간이 경과하기 전에 검증을 통과하지 못하기 때문에 취소됩니다. 실패: RFC가 실패했습니다. 실패 이유는 출력의 StatusReason을 참조하세요. AMS 작업은 자동으로 문제 티켓을 생성하고 필요에 따라 사용자와 통신합니다.

i Note

취소되거나 거부된 RFCs는 [UpdateRfc](#)를 사용하여 다시 제출할 수 있습니다. 단원을 참조하십시오 [RFCs 업데이트](#).

RFC가 필요한 모든 조건을 통과하면(예: 필요한 모든 파라미터가 지정됨) 상태가 로 변경됩니다 PendingApproval(자동 CTs도 승인이 필요하며 구문 및 파라미터 검사가 통과하면 자동으로 발생함). 전달되지 않으면 상태가 로 변경됩니다 Rejected. StatusReason는 거부에 대한 정보를 제공하고, ExecutionOutput 필드는 승인 및 완료에 대한 정보를 제공합니다. 오류 코드는 다음과 같습니다.

- InvalidRfcStateException: RFC가 호출된 작업을 허용하지 않는 상태입니다. 예를 들어 RFC가 제출된 상태로 전환된 경우 더 이상 수정할 수 없습니다.
- InvalidRfcScheduleException: StartTime, EndTime 또는 TimeoutInMinutes 파라미터가 위반되었습니다.
- InternalServerError: 시스템에 문제가 발생했습니다.
- InvalidArgumentException: 파라미터가 잘못 지정되었습니다. 예를 들어 허용할 수 없는 값이 사용되었습니다.
- ResourceNotFoundException: 스택 ID와 같은 값을 찾을 수 없습니다.

변경이 승인되기 전에 예약된 요청된 시작 및 종료 시간(변경 실행 기간이라고도 함)이 발생하면 RFC 상태가 로 변경됩니다 Canceled. 변경이 승인되면 RFC 상태가 로 변경됩니다 Scheduled. ASAP RFCs입니다. ExpectedExecutionDuration

변경 실행 기간이 도착하기 전에 언제든지 예약된 변경(CLIRequestedStartTime에서와 함께 제출됨)을 수정하거나 취소할 수 있습니다. 예약된 변경 사항이 수정되면 다시 제출해야 합니다.

변경 시작 시간이 도착하고(예약 또는 ASAP) 승인이 완료되면 상태가 로 변경 InProgress되며 수정할 수 없습니다. 지정된 변경 실행 기간 내에 변경이 완료되면 상태가 로 변경됩니다 Success. 변경의 일부가 실패하거나 변경 실행 기간이 종료될 때 변경 사항이 계속 진행 중인 경우 상태가 로 변경됩니다 Failure.

Note

InProgress, Success 또는 Failure 변경 상태 중에는 RFC를 수정하거나 취소할 수 없습니다.

다음 다이어그램은 CreateRFC 호출부터 해결까지의 RFC 상태를 보여줍니다.

RFC 업데이트 CTs 및 CloudFormation 템플릿 드리프트 감지 이해

AMS에 프로비저닝된 리소스는 수정된 AWS CloudFormation 템플릿을 사용합니다. 리소스에 서비스의 AWS Management Console을 통해 파라미터가 직접 변경된 경우 해당 리소스의 CloudFormation 생성 레코드가 동기화되지 않습니다. 이 경우 AMS 업데이트 변경 유형을 사용하여 AMS의 리소스를 업데이트하려고 하면 AMS는 원래 리소스 구성을 참조하고 잠재적으로 변경된 파라미터를 재설정합니다. 이 재설정은 손상될 수 있으므로 추가 AMS 구성 변경이 감지되면 AMS는 업데이트 변경 유형이 있는 RFCs를 허용하지 않습니다.

업데이트 변경 유형 목록은 콘솔 필터를 사용합니다.

드리프트 문제 해결 FAQs

AMS 드리프트 수정에 대한 질문과 답변. 드리프트 문제 해결을 시작하는 데 사용할 수 있는 두 가지 변경 유형이 있습니다. 하나는 실행 모드=수동 또는 "검토 필요"이고 다른 하나는 실행 모드=자동입니다.

드리프트 문제 해결 지원 리소스(ct-3kinq0u4l33zf)

드리프트 문제 해결 변경 유형(ct-3kinq0u4l33zf)에서 지원하는 리소스입니다. 리소스를 수정하려면 대신 "검토 필요"(ct-34sxf053yuzah) 변경 유형을 사용합니다.

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

드리프트 문제 해결 변경 유형

AMS 드리프트 문제 해결 변경 유형 사용에 대한 질문과 답변입니다.

드리프트 문제 해결 기능에 지원되는 리소스 목록은 섹션을 참조하세요 [드리프트 문제 해결 지원 리소스\(ct-3king0u4l33zf\)](#).

Important

드리프트 수정은 스택 템플릿 및/또는 파라미터를 수정하며, 최신 스택 템플릿 및 파라미터를 사용하도록 로컬 템플릿 리포지토리 또는 이러한 스택을 업데이트하는 자동화를 업데이트해야 합니다. 동기화 없이 이전 템플릿 및/또는 파라미터를 사용하면 기본 리소스가 손상될 수 있습니다.

검토가 필요하지 않은 자동 CT(ct-3king0u4l33zf)는 RFC당 10개의 리소스만 수정할 수 있도록 지원합니다. 나머지 리소스를 10개 배치로 수정하려면 모든 리소스가 수정될 때까지 새 RFCs 생성합니다.

어떤 드리프트 문제 해결 변경 유형을 사용해야 하나요?

다음과 같은 경우 검토가 필요 없는 자동 CT(ct-3king0u4l33zf)를 사용하는 것이 좋습니다.

- 자동 CT를 사용하여 기존 스택 리소스에 대한 업데이트를 수행하려고 하면 스택이 이므로 RFC가 거부됩니다 DRIFTED.
- 이전에 Update CT를 사용했는데 스택이 DRIFTED되어 실패했습니다. 업데이트를 다시 시도할 필요가 없으며 대신 필요한 검토, 수동, CT를 사용할 수 있습니다.

드리프트 문제 해결 검토 필요 없음, 자동, CT(ct-3king0u4l33zf) 또는 드리프트 문제 해결 필요 없음, 자동, CT 실패로 인해 드리프트 문제 해결이 지원되지 않는 경우에만 검토 필요, 수동 CT(ct-34sxf053yuzah)를 사용하는 것이 좋습니다.

문제 해결 중에 스택에 어떤 변경 사항이 적용되나요?

수정하려면 드리프트된 속성에 따라 스택 템플릿 및/또는 파라미터를 업데이트해야 합니다. 또한 문제 해결은 문제 해결 중에 스택의 스택 정책을 업데이트하고 문제 해결이 완료되면 스택 정책을 이전 값으로 복원합니다.

스택 템플릿 및/또는 파라미터에 수행된 변경 사항을 보려면 어떻게 해야 하나요?

RFC에 대한 응답으로 다음 정보와 함께 변경 요약이 제공됩니다.

- **ChangeSummaryJson**: 드리프트 수정의 일부로 스택 템플릿 및/또는 파라미터의 변경 요약을 포함합니다. 문제 해결은 여러 단계로 수행됩니다. 이 변경 요약은 개별 단계의 변경 사항으로 구성됩니다. 문제 해결이 성공하면 마지막 단계의 변경 사항을 확인합니다. 순서대로 실행되는 단계는 JSON의 ExecutionPlan을 참조하세요. 예를 들어, 있는 경우 RestoreReferences 섹션은 항상 끝에 실행되며 수정 후 변경 사항에 대한 JSON을 포함합니다. 문제 해결이 DryRun 모드에서 실행되는 경우 이러한 변경 사항 중 어떤 것도 스택에 적용되지 않았을 것입니다.
- **PreRemediationStackTemplateAndConfigurationJson**: 스택에서 수정이 트리거되기 전에 템플릿, 파라미터, 출력, StackPolicyBody를 포함한 CloudFormation 스택의 구성 스냅샷을 포함합니다.

문제 해결이 수행되면 어떻게 해야 하나요?

Important

로컬 템플릿 리포지토리 또는 수정 스택을 업데이트하는 자동화를 RFC 요약에 제공된 최신 템플릿 및 파라미터로 업데이트해야 합니다. 이전 템플릿 및/또는 파라미터를 사용하면 스택 리소스가 더 이상 파괴적으로 변경될 수 있으므로 이 작업을 수행하는 것이 매우 중요합니다.

이 문제 해결 중에 애플리케이션이 적용되나요?

해결은 CloudFormation 스택 구성에서만 수행되는 오프라인 프로세스입니다. 기본 리소스에 대한 업데이트는 수행되지 않습니다.

문제 해결 후 관리 | 기타 | 기타 RFCs 계속 사용하여 리소스에 대한 업데이트를 수행할 수 있습니까?

사용 가능한 자동 CTs 업데이트를 사용하여 스택 리소스에 대한 업데이트를 항상 수행하는 것이 좋습니다. 사용 가능한 CT 업데이트가 사용 사례를 지원하지 CTs 않는 경우 관리 | 기타 | 기타 요청을 사용합니다.

수정으로 스택에 새 리소스가 생성되나요?

수정은 스택에 새 리소스를 생성하지 않습니다. 그러나 수정은 새 출력을 생성하고 스택 템플릿 [메타데이터](#) 섹션을 업데이트하여 참조용으로 수정 요약을 저장합니다.

문제 해결은 항상 성공하나요?

수정을 수행하려면 템플릿 구성을 신중하게 분석하고 검증해야 합니다. 이러한 검증이 실패하는 시나리오에서는 수정 프로세스가 중지되고 스택 템플릿 또는 파라미터에 대한 변경 사항이 수행되지 않습니다. 또한 지원되는 리소스 유형에서만 문제 해결을 수행할 수 있습니다.

문제 해결에 실패하면 스택 리소스에 대한 업데이트를 수행하려면 어떻게 해야 합니까?

관리 | 기타 | 기타 | CT 업데이트(ct-0xdawir96cy7k)를 사용하여 변경을 요청할 수 있습니다. AMS는 이러한 시나리오를 모니터링하고 문제 해결 솔루션을 개선하기 위해 노력합니다.

지원되는 리소스 유형과 지원되지 않는 리소스 유형이 모두 있는 스택을 수정할 수 있나요?

예. 그러나 수정은 지원되는 리소스 유형이 스택에서 DRIFTED로 발견된 경우에만 수행됩니다. 지원되지 않는 리소스 유형이 DRIFTED인 경우 수정이 계속되지 않습니다.

비CFN Ingest CTs를 통해 생성된 스택에 대한 문제 해결을 요청할 수 있나요?

예. 스택 생성에 사용되는 변경 유형에 관계없이 스택에서 수정을 수행할 수 있습니다.

수정 전에 스택에 대해 수행할 변경 사항을 알 수 있나요?

예. 두 변경 유형 모두 스택이 수정될 경우 수행할 변경을 요청하는 데 사용할 수 있는 DryRun 옵션을 제공합니다. 그러나 최종 수정 변경 사항은 수정 시 스택에 있는 드리프트에 따라 다를 수 있습니다.

RFCs 예약

예약 기능을 사용하면 RFCs. 예약 기능에서 사용할 수 있는 옵션은 다음과 같습니다.

- 이 변경 사항을 최대한 빨리 실행: AMS는 RFC가 승인되는 즉시 실행합니다. 대부분의 CTs 자동으로 승인됩니다. RFC가 특정 시간에 시작되지 않도록 하려면이 옵션을 사용합니다.
- 이 변경 예약: RFC를 실행할 날짜, 시간 및 시간대를 설정합니다. 자동 변경 유형의 경우 RFC를 제출하려는 후 최소 10분 후에 시작 시간을 요청하는 것이 가장 좋습니다. 필수 변경 유형을 검토하려면 RFC를 제출하려는 후 최소 24시간이 지난 시작 시간을 요청해야 합니다. 구성된 시작 시간까지 RFC가 승인되지 않으면 RFC가 거부됩니다.

RFC 일정 설정

RFC를 예약하려면 다음 방법 중 하나를 사용합니다.

이 변경 사항을 최대한 빨리 실행합니다.

- 콘솔: 아무 작업도 수행하지 않습니다. 기본 RFC 일정을 사용합니다.
- API 또는 CLI: RFC 생성 작업에서 RequestedStartTime 및 RequestedEndTime 옵션을 제거합니다.

제출 후 30일 이내에 승인되지 않은 경우 ASAP "검토 필요" RFCs가 자동으로 거부됩니다.

이 변경 사항을 예약합니다.

- 콘솔: 이 변경 예약 라디오 버튼을 선택합니다. 시작 시간 영역이 열립니다. 수동으로 날짜를 입력하거나 일정 위젯을 사용하여 날짜를 선택합니다. ISO 8601 형식으로 표현된 시간을 UTC로 입력하고 드롭다운 목록을 사용하여 위치를 선택합니다. 기본적으로 AMS는 ISO 8601 형식 YYYYMMDDThhmmssZ 또는 YYYY-MM-DDThh:mm:ssZ를 사용하며, 두 형식 중 하나가 허용됩니다.

Note

기본 종료 시간은 입력한 시작 시간으로부터 4시간입니다. 예약된 변경의 종료 시간을 4시간 이상으로 설정하려면 API 또는 CLI를 사용하여 변경 사항을 실행합니다.

- API 또는 CLI: RFC 생성 작업에서 RequestedStartTime 및 RequestedEndTime 파라미터 값을 제출합니다. 구성된를 전달해도 이미 시작된 자동 변경 유형에 대한 실행이 중지RequestedEndTime되지 않습니다. '검토 필요' 변경 유형의 경우 AMS 운영 조사가 진행 중인 동안에 RequestedEndTime 도달하고 AMS와 통신하는 경우 확장을 요청하거나 RFC를 다시 제출하라는 메시지가 표시될 수 있습니다.

Tip

UTC 시간 읽기의 예는 Time-is 웹 사이트의 [UTC](#)를 참조하세요. 오후 2:20에 2016-12-05의 날짜/시간 값에 대한 ISO 8601 형식의 예: 2016-12-05T14:20:00Z 또는 20161205T142000Z.

제공하는 경우...

- 만RequestedStartTime, RFC는 예약된 것으로 간주되며 RequestedEndTime는 ExecutionDurationInMinutes 값을 사용하여 채워집니다.
- 만 해당됩니다. InvalidArgumentException이 RequestedEndTime발생합니다.
- RequestedStartTime 및 모두 RequestedEndTime 지정된 시작 시간 + ExecutionDurationInMinutes 값으로 RequestedEndTime덮어씁니다.
- RequestedStartTime 도 도 아닙니다. 이러한 값은 null로 RequestedEndTime유지되며 RFC는 ASAP RFC로 처리됩니다.

Note

예약된 모든 RFCs 대해 지정되지 않은 종료 시간은 지정된의 시간과 제출된 변경 유형의 RequestedStartTime ExpectedExecutionDurationInMinutes 속성으로 기록됩니다. 예를 들어 ExpectedExecutionDurationInMinutes가 "60"(분)이고 지정된 RequestedStartTime가 2016-12-05T14:20:00Z (2016년 12월 5일 오전 4시 20분)인 경우 실제 종료 시간은 2016년 12월 5일 오전 5시 20분으로 설정됩니다. 특정 변경 유형에 ExpectedExecutionDurationInMinutes 대한를 찾으려면 다음 명령을 실행합니다.

```
aws amscm --profile sam1 get-change-type-version --  
change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.  
{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

RFC 우선 순위 옵션 사용

execution mode = manual 변경 유형에서 우선 순위 옵션을 사용하여 AMS 작업에 요청의 긴급성을 알립니다.

의 우선 순위 옵션 execution mode = manual:

수동 RFC의 우선 순위를 높음, 중간 또는 낮음으로 지정합니다. 높음으로 분류된 RFCs는 RFCs 서비스 수준 목표(SLOs) 및 제출 시간에 따라 중간으로 분류된 RFC 이전에 검토 및 승인됩니다. 우선 순위가 낮거나 우선 순위가 지정되지 않은 RFCs는 제출된 순서대로 처리됩니다.

RFCs 승인 또는 거부

승인 필요(수동) CTs와 함께 제출된 RFCs는 사용자 또는 AMS의 승인을 받아야 합니다. 사전 승인된 CTs 자동으로 처리됩니다. 자세한 내용은 [CT 승인 요구 사항](#) 단원을 참조하십시오.

Note

'검토 필요' CTs를 사용하는 경우 ASAP 예약 옵션(콘솔에서 ASAP 선택, API/CLI에서 시작 및 종료 시간 비워 두기)을 사용하는 것이 좋습니다. 이러한 CTs는 AMS 운영자가 RFC를 검사하고 승인 및 실행 전에 사용자와 통신해야 하기 때문입니다. 이러한 RFCs 예약하는 경우 최소 24시간을 허용해야 합니다. 예약된 시작 시간 전에 승인이 이루어지지 않으면 RFC가 자동으로 거부됩니다.

AMS에서 승인 필요 RFC를 성공적으로 제출한 경우 사용자의 명시적 승인을 받아야 합니다. 또는 승인 필요 RFC를 제출하는 경우 AMS의 승인을 받아야 합니다. AMS가 제출한 RFC를 승인해야 하는 경우 승인을 요청하는 이메일 또는 기타 미리 결정된 통신이 전송됩니다. 통신에는 RFC ID가 포함됩니다. 통신이 전송된 후 다음 중 하나를 수행합니다.

- 콘솔 승인 또는 거부: 관련 RFC에 대한 RFC 세부 정보 페이지를 사용합니다.
- API/CLI 승인: [ApproveRfc](#)는 변경 사항을 승인됨으로 표시합니다. 필요한 경우 소유자와 운영자 모두 조치를 취해야 합니다. 다음은 CLI 승인 명령의 예입니다. 다음 예제에서는 RFC_ID를 적절한 RFC ID로 바꿉니다.

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- API/CLI 거부: [RejectRfc](#)는 변경 사항을 거부로 표시합니다. 다음은 CLI 거부 명령의 예입니다. 다음 예제에서는 RFC_ID를 적절한 RFC ID로 바꿉니다.

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

RFC 제한 실행 기간 요청

이전에는 블랙아웃 일수라고 했지만 특정 기간을 제한하도록 요청할 수 있습니다. 해당 시간 동안에는 변경 사항을 실행할 수 없습니다.

제한된 실행 기간을 설정하려면 [UpdateRestrictedExecutionTimes](#) API 작업을 사용하고 UTC로 특정 기간을 설정합니다. 지정한 기간은 지정된 이전 기간을 재정의합니다. 지정된 제한된 실행 시간 동안 RFC를 제출하면 잘못된 RFC 일정 오류와 함께 제출이 실패합니다. 최대 200개의 제한된 기간을 지정할 수 있습니다. 기본적으로 제한 기간은 설정되지 않습니다. 다음은 요청 명령의 예입니다(SAML 인증이 구성된 경우).

```
aws amscm --profile saml update-restricted-execution-times --restricted-execution-times='[{"TimeRange":{"StartTime":"2018-01-01T12:00:00Z","EndTime":"2018-01-01T12:00:01Z"}}]'
```

RestrictedExecutionTimes 설정을 볼 수도 있습니다. [ListRestrictedExecutionTimes](#) 예시

```
aws amscm --profile saml list-restricted-execution-times
```

지정된 제한된 실행 시간 동안 RFC를 제출하려면 `RestrictedExecutionTimesOverrideId`를 `OverrideRestrictedTimeRanges` 값으로 추가한 다음 평소와 같이 RFC를 제출합니다. 중요하거나 긴급한 RFC에만이 방법을 사용하는 것이 가장 좋습니다. 자세한 내용은 [SubmitRfc](#)에 대한 API 참조를 참조하세요.

RFCs 생성, 복제, 업데이트, 찾기 및 취소

다음 예제에서는 다양한 RFC 작업을 안내합니다.

주제

- [RFC 생성](#)
- [AMS 콘솔RFCs 복제\(다시 생성\)](#)
- [RFCs 업데이트](#)
- [RFCs 찾기](#)
- [RFCs 취소](#)

RFC 생성

콘솔을 사용하여 RFC 생성

다음은 AMS 콘솔에서 빠른 카드가 열려 있고 변경 유형 찾아보기가 활성화된 RFC 생성 프로세스의 첫 번째 페이지입니다.

다음은 범주별 선택이 활성화된 AMS 콘솔에서 RFC 생성 프로세스의 첫 번째 페이지입니다.

작동 방식:

1. RFC 생성 페이지로 이동합니다. AMS 콘솔의 왼쪽 탐색 창에서 RFCs 클릭하여 RFCs 목록 페이지를 연 다음 RFC 생성을 클릭합니다.
2. 기본 변경 유형 찾아보기 보기에서 인기 있는 변경 유형(CT)을 선택하거나 범주별 선택 보기에서 CT를 선택합니다.
 - 변경 유형별 찾아보기: 빠른 생성 영역에서 인기 있는 CT를 클릭하여 RFC 실행 페이지를 즉시 열 수 있습니다. 빠른 생성으로 이전 CT 버전을 선택할 수 없습니다.

CTs 정렬하려면 카드 또는 테이블 보기에서 모든 변경 유형 영역을 사용합니다. 어느 보기에서든 CT를 선택한 다음 RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다. 해당하는 경우 RFC 생성 버튼 옆에 이전 버전으로 생성 옵션이 나타납니다.

- 범주별 선택: 범주, 하위 범주, 항목 및 작업을 선택하면 해당하는 경우 이전 버전으로 생성 옵션이 있는 CT 세부 정보 상자가 열립니다. RFC 생성을 클릭하여 RFC 실행 페이지를 엽니다.

3. RFC 실행 페이지에서 CT 이름 영역을 열어 CT 세부 정보 상자를 확인합니다. 제목은 필수입니다 (변경 유형 찾아보기 보기에서 CT를 선택하면 입력됨). 추가 구성 영역을 열어 RFC에 대한 정보를 추가합니다.

실행 구성 영역에서 사용 가능한 드롭다운 목록을 사용하거나 필요한 파라미터의 값을 입력합니다. 선택적 실행 파라미터를 구성하려면 추가 구성 영역을 엽니다.

4. 완료되면 실행을 클릭합니다. 오류가 없는 경우 성공적으로 생성된 RFC 페이지에 제출된 RFC 세부 정보와 초기 실행 출력이 표시됩니다.
5. 실행 파라미터 영역을 열어 제출한 구성을 확인합니다. 페이지를 새로 고쳐 RFC 실행 상태를 업데이트합니다. 선택적으로 RFC를 취소하거나 페이지 상단의 옵션을 사용하여 RFC 사본을 생성합니다.

CLI를 사용하여 RFC 생성

작동 방식:

1. 인라인 생성(모든 RFC 및 실행 파라미터가 포함된 `create-rfc` 명령을 실행) 또는 템플릿 생성(2개의 JSON 파일을 생성, 하나는 RFC 파라미터용이고 다른 하나는 실행 파라미터용)을 사용하고 두 파일을 입력으로 사용하여 `create-rfc` 명령을 실행합니다. 두 방법 모두 여기에 설명되어 있습니다.
2. 반환된 RFC ID로 RFC: `aws amscm submit-rfc --rfc-id ID` 명령을 제출합니다.

RFC: `aws amscm get-rfc --rfc-id ID` 명령을 모니터링합니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=CT_ID
```

Note

변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 RFC에서 CreateRfc 파라미터를 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 --notification '{"Email\\": {"EmailRecipients\\": [{"email@example.com\\"}]}}' RFC 파라미터 부분(실행 파라미터 아님)에이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 [AMS Change Management API 참조](#)를 참조하세요.

인라인 생성:

인라인으로 제공된 실행 파라미터(실행 파라미터를 인라인으로 제공할 때 따옴표 이스케이프)로 RFC 생성 명령을 실행한 다음 반환된 RFC ID를 제출합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title "TITLE" --execution-parameters "{\"Description\\": \"example\\\"}"
```

템플릿 생성:**Note**

RFC를 생성하는 이 예제에서는 Load Balancer(ELB) 스택 변경 유형을 사용합니다.

1. 관련 CT를 찾습니다. 다음 명령은 항목 이름에 "ELB"가 포함된 CT 분류 요약を検査하고 범주, 항목, 작업 및 ChangeTypeId의 출력을 테이블 형식으로 생성합니다(둘 다 하위 범주는 Advanced stack components).

```
aws amscm list-change-type-classification-summaries --query "ChangeTypeClassificationSummaries[?contains(Item, 'ELB')]. [Category, Item, Operation, ChangeTypeId]" --output table
```

```
-----
|                               CtSummaries                               |
+-----+-----+-----+-----+
| Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7j1 |
| Management| Load balancer (ELB) stack | Update | ct-01tm873rseb9  |
+-----+-----+-----+-----+
```

```
+-----+-----+-----+-----+
```

2. 최신 버전의 CT를 찾습니다.

ChangeTypeId 및 ChangeTypeVersion: 이 연습의 변경 유형 ID는 ct-123h45t6uz7j1 (ELB 생성)입니다. 최신 버전을 확인하려면 다음 명령을 실행합니다.

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=ct-123h45t6uz7j1
```

3. 옵션 및 요구 사항을 알아봅니다. 다음 명령은 스키마를 CreateElbParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7j1" --query
"ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. 실행 파라미터 JSON 파일을 수정하고 저장합니다. 이 예제에서는 CreateElbParams.json.

프로비저닝 CT의 경우 StackTemplateId는 스키마에 포함되며 실행 파라미터에 제출해야 합니다.

TimeoutInMinutes의 경우 RFC가 실패하기 전에 스택을 생성하는 데 허용되는 분 수는 이 설정으로 인해 RFC 실행이 지연되지 않지만 충분한 시간을 제공해야 합니다(예: "5"를 지정하지 않음). UserData: Create EC2 and Create ASG가 장기 실행되는 CTs 경우 유효한 값은 "60"~"360"입니다. 다른 모든 프로비저닝 CTs에 허용되는 최대 "60"을 권장합니다.

스택을 생성할 VPC의 ID를 입력합니다. CLI 명령을 사용하여 VPC ID를 가져올 수 있습니다 `aws amsskms list-vpc-summaries`.

```
{
  "Description":      "ELB-Create-RFC",
  "VpcId":            "VPC_ID",
  "StackTemplateId":  "stm-sdhopv000000000000",
  "Name":             "MyElbInstance",
  "TimeoutInMinutes": 60,
  "Parameters": {
    "ELBSubnetIds":    ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold": 4,
    "ELBHealthCheckInterval": 5,
    "ELBHealthCheckTarget": "HTTP:80/",
    "ELBHealthCheckTimeout": 60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":       false
  }
}
```

```
}
```

5. RFC JSON 템플릿을 CreateElbRfc.json이라는 현재 폴더의 파일로 출력합니다.

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. CreateElbRfc.json 파일을 수정하고 저장합니다. 별도의 파일에서 실행 파라미터를 생성했으므로 ExecutionParameters 줄을 제거합니다. 예를 들어 콘텐츠를 다음과 같은 내용으로 바꿀 수 있습니다.

```
{
  "ChangeTypeVersion":    "2.0",
  "ChangeTypeId":         "ct-123h45t6uz7jl",
  "Title":                "Create ELB"
}
```

7. RFC를 생성합니다. 다음 명령은 실행 파라미터 파일과 RFC 템플릿 파일을 지정합니다.

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-parameters file://CreateElbParams.json
```

응답에서 새 RFC의 ID를 수신하고 이를 사용하여 RFC를 제출하고 모니터링할 수 있습니다. 제출하기 전까지는 RFC가 편집 상태로 유지되고 시작되지 않습니다.

팁

Note

AMS API/CLI를 사용하여 RFC JSON 파일 또는 CT 실행 파라미터 JSON 파일을 생성하지 않고도 RFC를 생성할 수 있습니다. 이렇게 하려면 create-rfc 명령을 사용하고 필요한 RFC 및 실행 파라미터를 명령에 추가합니다. 이를 "인라인 생성"이라고 합니다. 모든 프로비저닝 CTs 리소스에 대한 파라미터가 포함된 Parameters 배열이 execution-parameters 블록 내에 포함되어 있습니다. 파라미터에는 슬래시(/)로 이스케이프된 따옴표가 있어야 합니다. RFC를 생성하는 다른 문서화된 방법을 "템플릿 생성"이라고 합니다. 여기에서 RFC 파라미터에 대한 JSON 파일과 실행 파라미터에 대한 다른 JSON 파일을 생성하고 create-rfc 명령을 사용하여 두 파일을 제출합니다. 이러한 파일은 템플릿 역할을 할 수 있으며 향후 RFCs. 템플릿을 사용하여 RFCs를 생성할 때 명령을 사용하여 다음과 같이 명령을 실행하여 원하는 콘텐츠로 JSON 파일을 생성할 수 있습니다. 명령은 표시된 콘텐츠와 함께

"parameters.json"이라는 파일을 생성합니다. 이러한 명령을 사용하여 RFC JSON 파일을 생성할 수도 있습니다.

AMS 콘솔RFCs 복제(다시 생성)

AMS 콘솔을 사용하여 기존 RFC를 복제할 수 있습니다.

AMS 콘솔을 사용하여 RFC를 복제하거나 다시 생성하려면 다음 단계를 따르세요.

1. 관련 RFC를 찾습니다. 왼쪽 탐색 창에서 RFCs 클릭합니다.

RFCs 열립니다.

2. 복제하려는 RFC를 찾을 때까지 페이지를 스크롤합니다. 필터 옵션을 사용하여 목록의 범위를 좁힙니다. 복제할 RFC를 선택합니다.

RFC 세부 정보 페이지가 열립니다.

3. 복사본 생성을 클릭합니다.

변경 요청 생성 페이지가 열리고 모든 옵션이 원래 RFC에서 로 설정됩니다.

4. 원하는 대로 변경합니다. 추가 옵션을 설정하려면 기본 옵션을 고급으로 변경합니다. 모든 옵션을 설정한 후 제출을 선택합니다.

활성 RFC 세부 정보 페이지가 복제된 RFC의 새 RFC ID와 함께 열리고 복제된 RFC가 RFC 대시 보드에 나타납니다.

RFCs 업데이트

RFC를 업데이트한 다음 제출하거나 다시 제출하여 거부되었거나 아직 제출되지 않은 RFC를 다시 제출할 수 있습니다. 지정된 RFCsRequestedStartTime가 제출 전에 통과했거나 지정된 TimeoutInMinutes가 RFC를 실행하기에 충분하지 않기 때문에 대부분의 RFC가 거부됩니다 (TimeoutInMinutes는 성공적인 RFC를 연장하지 않으므로 Amazon EC2 또는 장기 실행 UserData가 있는 Amazon EC2 Auto Scaling 그룹의 경우 항상 "60"~"360"으로 설정하는 것이 좋습니다). 이 섹션에서는 CLI 버전의 UpdateRfc 명령을 사용하여 새 RFC 파라미터로 RFC를 업데이트하거나 문자열화된 JSON 또는 업데이트된 파라미터 파일을 사용하여 새 파라미터를 업데이트하는 방법을 설명합니다.

이 예제에서는 AMS UpdateRfc API의 CLI 버전 사용에 대해 설명합니다([RFC 업데이트](#) 참조). 일부 리소스(DNS 프라이빗 및 퍼블릭, 로드 밸런서 스택 및 스택 패치 구성)를 업데이트하기 위한 변경 유형이 있지만 RFC를 업데이트할 CT는 없습니다.

한 번에 하나의 UpdateRfc 작업을 제출하는 것이 좋습니다. 예를 들어 DNS 스택에서 여러 업데이트를 제출하면 업데이트가 DNS를 동시에 업데이트하지 못할 수 있습니다.

필수 데이터: RfcId: 업데이트 중인 RFC입니다.

선택적 데이터: ExecutionParameters와 같이 필요하지 않은 필드를 업데이트하지 않는 한 수정된 실행 파라미터를 Description 제출하여 RFC가 거부되거나 취소되는 문제를 해결합니다. 제출된 모든 null이 아닌 값은 원래 RFC에서 해당 값을 덮어씁니다.

1. 거부되거나 취소된 관련 RFC를 찾으려면 명령을 사용할 수 있습니다(값을 로 대체할 수 있음Canceled).

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
```

2. 다음 RFC 파라미터 중 하나를 수정할 수 있습니다.

```
{
  "Description": "string",
  "ExecutionParameters": "string",
  "ExpectedOutcome": "string",
  "ImplementationPlan": "string",
  "RequestedEndTime": "string",
  "RequestedStartTime": "string",
  "RfcId": "string",
  "RollbackPlan": "string",
  "Title": "string",
  "WorstCaseScenario": "string"}
```

설명 필드를 업데이트하는 명령의 예:

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
--region us-east-1
```

ExecutionParameters VpcId 필드를 업데이트하는 명령 예제:

```
aws amscm update-rfc --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
"RFC_ID" --region us-east-1
```

업데이트가 포함된 실행 파라미터 파일로 RFC를 업데이트하는 명령 예제. [EC2 스택 | 생성](#)의 2단계에서 실행 파라미터 파일 예제 참조:

```
aws amscm update-rfc --execution-parameters file:///CreateEc2ParamsUpdate.json --  
rfc-id "RFC_ID" --region us-east-1
```

3. RFC를 처음 생성할 때와 동일한 RFC IDsubmit-rfc를 사용하여 RFC를 다시 제출합니다.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

RFC가 성공하면 명령줄에 확인 또는 오류 메시지가 표시되지 않습니다.

4. 요청 상태를 모니터링하고 실행 출력을 보려면 다음 명령을 실행합니다.

```
aws amscm get-rfc --rfc-id RFC_ID
```

RFCs 찾기

콘솔을 사용하여 변경 요청(RFC) 찾기

AMS 콘솔을 사용하여 RFC를 찾으려면 다음 단계를 따르세요.

Note

이 절차는 예약된 RFCs, 즉 ASAP 옵션을 사용하지 않은 RFCs에만 적용됩니다.

1. 왼쪽 탐색 창에서 RFCs 클릭합니다.

RFCs 열립니다.

2. 목록을 스크롤하거나 필터 옵션을 사용하여 목록을 구체화합니다.

RFC 목록은 필터 기준에 따라 변경됩니다.

3. 원하는 RFC의 제목 링크를 선택합니다.

RFC ID를 포함한 정보가 포함된 해당 RFC에 대한 RFC 세부 정보 페이지가 열립니다.

4. 대시보드에 RFCs가 많은 경우 필터 옵션을 사용하여 RFC로 검색할 수 있습니다.

- 제목: 생성 시 RFC에 제공된 제목 줄 또는 제목(API/CLI).
- RFC ID: RFC의 식별자입니다.

- **활동 상태:** RFC 상태를 알고 있는 경우 운영자가 현재 RFC를 보고 있다는 의미의 `AwsOperatorAssigned`, RFC 실행을 진행하기 전에 AMS 운영자가 무언가를 수행해야 한다는 의미의 `AwsActionPending` 또는 RFC 실행을 진행하기 전에 조치를 취해야 한다는 의미의 `CustomerActionPending` 중에서 선택할 수 있습니다.
- **상태:** RFC 상태를 알고 있는 경우 다음 중에서 선택할 수 있습니다.
 - **예약됨:** 예약된 RFCs.
 - **취소됨:** 취소된 RFCs.
 - **진행 중:** RFCs 진행 중입니다.
 - **성공:** 성공적으로 실행된 RFCs.
 - **거부됨:** 거부된 RFCs.
 - **편집:** 편집 중인 RFCs.
 - **Failure:** 실패한 RFCs.
 - **승인 보류 중:** AMS 또는 사용자가 승인할 때까지 진행할 수 없는 RFCs. 일반적으로 이는 RFC를 승인해야 함을 나타냅니다. 서비스 요청 목록에서 이에 대한 서비스 알림을 받게 됩니다.
- **변경 유형:** 범주, 하위 범주, 항목 및 작업을 선택하면 변경 유형 ID가 검색됩니다.
- **요청된 시작 시간 또는 요청된 종료 시간:** 이 필터 옵션을 사용하면 이전 또는 이후를 선택한 다음 날짜 및 선택적으로 시간(hh:mm 및 시간대)을 입력할 수 있습니다. 이 필터는 예약된 RFCs(ASAP RFCs 아님)에서만 성공적으로 작동합니다.
- **상태:** 예약됨, 취소됨, 진행 중, 성공, 거부됨, 편집 중 또는 실패.
- **제목:** RFC에 제공한 제목(또는 RFC가 API/CLI로 생성된 경우 제목)입니다.
- **변경 유형 ID:** RFC와 함께 제출된 변경 유형의 식별자를 사용합니다.

다음 스크린샷과 같이 검색을 통해 필터를 추가할 수 있습니다.

5. 원하는 RFC의 제목 링크를 클릭합니다.

RFC ID를 포함한 정보가 포함된 해당 RFC에 대한 RFC 세부 정보 페이지가 열립니다.

CLI를 사용하여 변경 요청(RFC) 찾기

여러 필터를 사용하여 RFC를 찾을 수 있습니다.

변경 유형 버전을 확인하려면 다음 명령을 사용합니다.


```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=CT_ID
```

Note

변경 유형에 대한 스키마의 일부인지 여부에 관계없이 모든 CreateRfc 파라미터를 RFC와 함께 사용할 수 있습니다. 예를 들어 RFC 상태가 변경될 때 알림을 받으려면 요청의 --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\" RFC 파라미터 부분(실행 파라미터 아님)에 이 줄을 추가합니다. 모든 CreateRfc 파라미터 목록은 [AMS Change Management API 참조](#)를 참조하세요.

RFC ID를 기록하지 않고 나중에 찾아야 하는 경우 AMS 변경 관리(CM) 시스템을 사용하여 이를 검색하고 필터 또는 쿼리로 결과의 범위를 좁힐 수 있습니다.

1. CM API [ListRfcSummaries](#) 작업에는 필터가 있습니다. 논리적 AND 작업에서 Attribute 및 Value 결합하거나, Condition 및 Attribute를 기반으로 결과를 [필터링](#)할 수 있습니다Values.

RFC 필터링

속성	유효값	유효한 조건	기본 조건	참고
ActualEndTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: "20170101T000000Z")	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값 이전의 날짜를 나타내야 합니다.
ActualStartTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: "20170101T000000Z")	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드

속성	유효값	유효한 조건	기본 조건	참고
				에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값 이전의 날짜를 나타내야 합니다.
AutomationStatusId	수동, 자동	같음	같음	자동화 상태는 두 개 뿐입니다.
ChangeTypeId	유효한 변경 유형 ID. 예: ct-123h45t6uz7jl	같음	같음	변경 유형 또는 CSIO 찾기
ChangeTypeVersion	유효한 변경 유형 ID. 예: 1.0	같음	같음	변경 유형 또는 CSIO 찾기
CreatedBy	모든 문자열(최대 허용 길이는 2048자)	포함	포함	RFC의 CreatedBy 필드에는 RFC를 생성한 사용자의 ARNO이 포함됩니다.
CreatedTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: "20170101T000000Z")	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값 이전의 날짜를 나타내야 합니다.

속성	유효값	유효한 조건	기본 조건	참고
LastModifiedTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: "20170101T000000Z")	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값 이전의 날짜를 나타내야 합니다.
LastSubmittedTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: "20170101T000000Z")	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값 이전의 날짜를 나타내야 합니다.
RequestedEndTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: "20170101T000000Z")	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값 이전의 날짜를 나타내야 합니다.

속성	유효값	유효한 조건	기본 조건	참고
RequestedStartTime	ISO8601 날짜/시간을 나타내는 모든 문자열(예: “20170101T000000Z”)	이전, 이후, 사이	없음	이전 또는 이후 조건은 값 필드에 하나의 값만 허용합니다. 사이 조건에는 값 필드에 정확히 두 개의 값이 있어야 합니다. 여기서 첫 번째 값은 두 번째 값 이전의 날짜를 나타내야 합니다.
RfcStatusId	취소됨, 편집 중, 실패, InProgress, PendingApproval 중, 거부됨, 예약됨, 성공	같음	같음	AMS 콘솔에서 RFC 목록을 새로 고치거나 GetRfc 를 실행합니다.
Title	유효한 RFC 제목	포함	포함	각 개별 필드의 정규식은 지원되지 않습니다. 대/소문자를 구분하지 않는 검색

예시:

SQS와 관련된 모든 RFCs의 IDs를 찾으려면(SQS가 CT의 항목 부분에 포함된 경우) 다음 명령을 사용할 수 있습니다.

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

다음과 같은 결과를 반환합니다.

```
-----
|                               ListRfcSummaries                               |
+-----+-----+-----+-----+-----+-----+
|Deployment| Advanced Stack Components |SQS   |Create |ct-123h45t6uz7j1|
|Management| Monitoring & Notifcation  |SQS   |Update |ct-123h45t6uz7j1|
```

+-----+-----+-----+-----+-----+-----+

에 사용할 수 있는 또 다른 필터 `list-rfc-summaries`는 자동 또는 수동 RFCs Automation Status Id를 찾는입니다.

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

에 사용할 수 있는 또 다른 필터 `list-rfc-summaries`는 Title (콘솔의 제목)입니다.

```
Attribute=Title,Value=RFC-TITLE
```

RFCs:

- (제목에는 "Windows 2012" 또는 "Amazon Linux"라는 문구가 포함되어 있음) 및
- (RfcStatusId EQUALS "Success" 또는 "InProgress") AND
- (20170101T000000Z <= RequestedStartTime <= 20170103T000000Z) AND (ActualEndTime <= 20170103T000000Z)

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

```

    }
  ]
}
```

Note

고급을 통해 FiltersAMS는 향후 릴리스에서 다음 필드를 더 이상 사용하지 않으려고 합니다.

- 값: 값 필드는 필터 필드의 일부입니다. 고급 기능을 지원하는 값 필드를 사용합니다.
- RequestedEndTimeRange: 고급 기능을 지원하는 필터 필드 내에서 RequestedEndTime 사용
- RequestedStartTimeRange: 고급 기능을 지원하는 필터 필드 내에서 RequestedStartTime를 사용합니다.

CLI 쿼리 사용에 대한 자세한 내용은 [--query 옵션을 사용하여 출력을 필터링하는 방법](#) 및 쿼리 언어 참조인 [JMESPath 사양](#)을 참조하세요.

2. AMS 콘솔을 사용하는 경우:

RFCs 페이지로 이동합니다. 필요한 경우 RFC 주체를 기준으로 필터링할 수 있습니다. RFC 주체는 RFC를 생성할 Title 때 RFC로 입력한 것입니다.

팁

Note

이 절차는 예약된 RFCs, 즉 ASAP 옵션을 사용하지 않은 RFCs에만 적용됩니다.

RFCs 취소

콘솔 또는 AMS API/CLI를 사용하여 RFC를 취소할 수 있습니다.

콘솔을 사용하여 RFC를 취소하려면 RFC 목록에서 RFC를 찾아 열고 취소를 클릭합니다.

필수 데이터:

- Reason: RFC를 취소하는 이유.

- RfcId: 취소하려는 RFC입니다.

1. 일반적으로 RFC를 제출한 직후 취소합니다(RFC ID가 유용해야 함). 그렇지 않으면 예약한 후 지정된 시작 시간 이전이 아니면 취소할 수 없습니다. RFC ID를 찾아야 하는 경우 이 명령을 사용할 수 있습니다(수동으로 승인된 RFC를 PendingApproval Value로 대체할 수 있음).

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
```

2. RFC를 취소하는 명령의 예:

```
aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --region us-east-1
```

RFCs와 함께 AMS 콘솔 사용

AMS 콘솔은 RFCs를 생성하고 제출하는 데 도움이 되는 기능을 제공합니다.

RFC 목록 페이지 사용(콘솔)

AMS 콘솔 RFCs 목록 페이지에는 다음 옵션이 제공됩니다.

- 필터를 통한 고급 RFC 검색. 자세한 내용은 [RFCs 찾기](#) 단원을 참조하세요.
- RFC가 마지막으로 수정된 시간을 찾습니다. 이 값은 RFC 상태가 마지막으로 변경된 시간을 나타냅니다.
- RFC 주체를 사용하여 RFC 세부 정보 보기. 이 링크를 선택하면 해당 RFC의 세부 정보 페이지가 열립니다.
- RFC 상태 보기. 자세한 정보는 [RFC 상태 코드 이해](#) 섹션을 참조하세요.

RFC 빠른 생성 사용(콘솔)

RFC 빠른 생성 카드 또는 목록 테이블을 사용하거나 분류별로 RFCs에 대한 변경 유형을 선택합니다.

자세한 내용은 [RFC 생성](#)를 참조하세요.

RFC 서신 및 첨부 파일 추가(콘솔)

예를 들어 "PendingApproval" 상태일 때 RFC가 제출된 후 승인되기 전에 RFC에 서신을 추가할 수 있습니다. RFC가 승인된 후("예약됨" 또는 "InProgress" 상태) 요청에 대한 변경으로 해석될 수 있으므로 서신을 추가할 수 없습니다. RFC가 완료된 후("Canceled", "Rejected", "Success" 또는 "Failure" 상태) RFC가 30일 이상 닫히면 대응이 비활성화되지만 대응이 다시 활성화됩니다.

Note

각 서신은 5,000자로 제한됩니다.

첨부 파일에 대한 제한 사항:

- 서신당 첨부 파일은 3개뿐입니다.
- RFC당 첨부 파일을 50개로 제한합니다.
- 각 연결의 크기는 5MB 미만이어야 합니다.
- 일반 텍스트(.txt), 쉼표로 구분된 값(.csv), JSON(.json) 또는 YAML()과 같은 텍스트 파일만 허용됩니다.yaml. YAML 형식의 경우 파일 확장자를 사용하여 파일을 첨부해야 합니다.yaml.

Note

XML 콘텐츠가 있는 텍스트 파일은 금지됩니다. AMS와 공유할 XML 콘텐츠가 있는 경우 서비스 요청을 사용합니다.

- 파일 이름은 숫자, 문자, 공백, 대시(-), 밑줄(_), 점(.)만 포함하여 255자로 제한됩니다.
- RFC에서 첨부 파일을 업데이트하고 삭제하는 것은 현재 지원되지 않습니다.

RFC에 서신과 첨부 파일을 추가하려면 다음 단계를 따르세요.

1. AMS 콘솔의 RFC 세부 정보 페이지에서 페이지 하단의 서신 섹션을 찾습니다.

서신을 보내기 전에:

일부 서신을 보낸 후:

2. 새 서신을 추가하려면 회신 텍스트 상자에 메시지를 입력합니다. 서신과 관련된 파일을 첨부하려면 첨부 파일 추가를 선택한 다음 원하는 파일을 선택합니다.
3. 완료되면 제출을 선택합니다.

새 서신은 첨부된 파일에 대한 링크와 함께 RFC 세부 정보 페이지의 서신 목록에 표시됩니다.

RFC 이메일 알림 구성(콘솔)

AMS 콘솔 변경 요청 생성 페이지에서는 이메일 주소를 추가하여 RFC 상태 변경 알림을 받을 수 있습니다.

또한 다음과 같은 모든 변경 유형에 알림의 이메일 주소를 추가할 수 있습니다.

```
aws amscm create-rfc --change-type-id <Change type ID>
                    --change-type-version 1.0 --title "TITLE"
                    --notification "{\"Email\": {\"EmailRecipients\" :
[\"email@example.com\"]}}\""
```

파라미터 부분이 아닌 요청의 RFC 파라미터 부분에 있는 모든 변경 유형 인라인 또는 템플릿 요청에 유사한 줄(--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\")을 추가합니다.

일반적인 RFC 파라미터에 대해 알아보기

다음은 제출해야 하는 RFC 파라미터와 RFCs

- 변경 유형 정보: ChangeTypeId 및 ChangeTypeVersion. 변경 유형 IDs. <https://docs.aws.amazon.com/managedservices/latest/ctref/index.html>

query 인수를 사용하여 `CLIlst-change-type-classification-summaries`에서 실행하여 결과의 범위를 좁힙니다. 예를 들어, 결과를 좁혀 Item 이름에 "Access"가 포함된 유형을 변경합니다.

```
aws amscm list-change-type-classification-summaries --query
"ChangeTypeClassificationSummaries [?contains (Item, 'access')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

를 실행 `get-change-type-version` 하고 변경 유형 ID를 지정합니다. 다음 명령은 `ct-2tylseo8rxfsc`의 CT 버전을 가져옵니다.

```
aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
```

- 제목: RFC의 이름입니다. 이 이름은 AMS 콘솔 RFC 목록에서 RFC의 주체가 되며 `GetRfc` 명령과 필터를 사용하여 검색할 수 있습니다. Title
- 예약: 예약된 RFC를 원하는 경우 `RequestedStartTime` 및 `RequestedEndTime` 파라미터를 포함하거나 이 변경 예약 콘솔 옵션을 사용해야 합니다. ASAP RFC(승인되는 즉시 실행)의 경우 CLI를 사용할 때 `RequestedStartTime` 및 `RequestedEndTime` null을 그대로 둡니다. 콘솔을 사용할 때 ASAP 옵션을 수락합니다.

`RequestedStartTime`이 누락된 경우 RFC가 거부됩니다.

- 프로비저닝 CTs: 실행 파라미터 또는 `Parameters`는 리소스를 프로비저닝하는 데 필요한 특정 설정입니다. CT에 따라 크게 달라집니다.
- 비프로비저닝 CTs: CTs 또는 기타 | 기타 또는 스택 삭제와 같이 리소스를 프로비저닝하지 않는 CTs에는 최소한의 실행 파라미터가 있으며 `Parameters` 블록이 없습니다.
- 또한 일부 RFCs에서는 `TimeoutInMinutes`를 지정하거나 RFC가 실패하기 전에 스택을 생성하는 데 허용되는 분 수를 지정해야 합니다. 유효한 값은 장기 실행 `UserData`의 경우 60(분)~360입니다. 이 `TimeoutInMinutes` 초과되기 전에 실행을 완료할 수 없는 경우 RFC가 실패합니다. 그러나 이 설정은 RFC 실행을 지연시키지 않습니다.
- S3 버킷 또는 ELB와 같이 인스턴스를 생성하는 RFCs는 일반적으로 최대 7개의 태그(키/값 페어)를 추가할 수 있는 스키마를 제공합니다. 배포 | 고급 스택 구성 요소 | 태그 | 변경 유형 생성 (`ct-3cx7we852p3af`)을 사용하여 RFC를 제출하여 S3 버킷에 태그를 더 추가할 수 있습니다. EC2, EFS, RDS 및 다중 계층(HA 2계층 및 HA 1계층) 스키마는 최대 50개의 태그를 허용합니다. 태그는 스키마의 `ExecutionParameters` 부분에 지정됩니다. 태그를 제공하는 것은 큰 가치가 있을 수 있습니다. 자세한 내용은 [Amazon EC2 리소스에 태그 지정](#) 단원을 참조하십시오.

AMS 콘솔을 사용하는 경우 태그를 추가하려면 추가 구성 영역을 열어야 합니다.

Tip

많은 CT 스키마에는 스키마 상단에 `Description` 및 `Name` 필드가 있습니다. 이러한 필드는 스택 또는 스택 구성 요소의 이름을 지정하는 데 사용되며, 생성 중인 리소스의 이름은 지정하지 않습니다. 일부 스키마는 생성 중인 리소스의 이름을 지정하는 파라미터를 제공하고 일부는 그렇지 않습니다. 예를 들어 EC2 스택 생성을 위한 CT 스키마는 EC2 인스턴스 이름

을 지정하는 파라미터를 제공하지 않습니다. 이렇게 하려면 "Name" 키와 이름을 지정할 값을 사용하여 태그를 생성해야 합니다. 이러한 태그를 생성하지 않으면 EC2 인스턴스가 이름 속성 없이 EC2 콘솔에 표시됩니다.

RFC AWS 리전 옵션 사용

AMS API 및 CLI(amscm 및 amsskms) 엔드포인트에는 있습니다 us-east-1. SAML(Security Assertion Markup Language)과 연동하면 온보딩 시 AWS 리전을 us-east-1로 설정하는 스크립트가 제공됩니다. SAML을 사용하는 경우 명령을 실행할 때 --region 옵션을 지정할 필요가 없습니다. SAML이 us-east-1을 사용하도록 구성되어 있지만 계정이 해당 AWS 리전에 없는 경우 다른 AWS 명령(예:)을 실행할 때 계정 온보딩 리전을 지정해야 합니다 aws s3.

Note

이 가이드에 제공된 대부분의 명령 예제에는 --region 옵션이 포함되어 있지 않습니다.

RFC 일일 이메일에 가입

RFC 다이제스트 기능을 사용하여 지난 24시간 동안 계정의 RFC 활동을 요약하는 일일 이메일에 가입할 수 있습니다. RFC 다이제스트 기능은 계정의 RFCs. RFC 다이제스트는 응답을 보류 중인 작업을 놓칠 가능성을 줄일 수 있습니다.

RFC 다이제스트 기능을 켜려면 AMS Cloud Service Delivery Manager(CSDM)에 문의하세요. CSDM에서 구독합니다. RFC 다이제스트 이메일 목록에 포함할 이메일 주소(또는 별칭)를 최대 20개까지 요청할 수 있습니다. 현재 이메일 일정은 09:00 UTC-8에 고정됩니다.

RFC 다이제스트 기능을 끄려면 요청과 함께 CSDM에 문의하세요.

RFC 다이제스트를 설정하지 않고 RFCs에 대한 알림을 원하는 경우 또는 RFCs 다이제스트가 제공하는 것보다 RFC에 대한 자세한 정보를 원하는 경우 변경 관리 시스템을 사용하여 정보를 원하는 모든 개별 RFC에 대해 CloudWatch Events 알림 또는 이메일 알림을 설정합니다. RFC 알림 설정에 대한 자세한 내용은 [RFC 상태 변경 알림을 참조하세요](#).

RFC 다이제스트에 포함된 주제는 다음과 같습니다.

- 고객 승인 대기 중: 승인 대기 PendingApproval 상태인 RFCs를 나열합니다.
- 고객 응답 대기 중: RFCs 서신에 대한 응답을 기다리고 있는 RFC를 나열합니다.

- AWS 승인 또는 회신 보류 중: AMS에서 회신 또는 승인을 기다리고 있는 RFCs 나열합니다.
- 완료됨: 성공, 실패, 취소됨 및 거부됨 상태의 RFCs를 나열합니다.

다음은 RFC 다이제스트의 예입니다.

변경 유형이란 무엇입니까?

변경 유형은 AWS Managed Services(AMS)의 변경 요청(RFC)이 수행하고 변경 작업 자체와 수동 및 자동의 변경 유형을 포함하는 작업을 나타냅니다. AMS에는 다른 Amazon 웹 서비스에서 사용하지 않는 대규모 변경 유형 모음이 있습니다. 리소스 배포, 관리 또는 액세스 권한을 얻기 위해 변경 요청(RFC)을 제출할 때 이러한 변경 유형을 사용합니다.

주제

- [자동 및 수동 CTs](#)
- [CT 승인 요구 사항](#)
- [유형 버전 변경](#)
- [변경 유형 생성](#)
- [변경 유형 업데이트](#)
- [내부 전용 변경 유형](#)
- [변경 유형 스키마](#)
- [변경 유형에 대한 권한 관리](#)
- [변경 유형에서 민감한 정보 수정](#)
- [쿼리 옵션을 사용하여 변경 유형 찾기](#)

자동 및 수동 CTs

변경 유형에 대한 제약 조건은 자동 또는 수동인지 여부입니다. 이는 AMS 콘솔에서 실행 모드라고 하는 변경 유형 AutomationStatusId 속성입니다.

자동 변경 유형은 예상 결과와 실행 시간이 있으며 일반적으로 1시간 이내에 AMS 자동 시스템을 통해 실행됩니다(대부분 CT가 프로비저닝하는 리소스에 따라 다름). 수동 변경 유형은 흔하지 않지만 AMS 연산자가 실행되기 전에 RFC에서 작업해야 하므로 다르게 처리됩니다. 이는 RFC 제출자와 통신하는 것을 의미하기도 하므로 수동 변경 유형을 완료하려면 다양한 시간이 필요합니다.

예약된 모든 RFCs 대해 지정되지 않은 종료 시간은 지정된의 시간과 제출된 변경 유형의 RequestedStartTime ExpectedExecutionDurationInMinutes 속성으로 기록됩니다. 예를 들어 ExpectedExecutionDurationInMinutes가 "60"(분)이고 지정된 RequestedStartTime가 2016-12-05T14:20:00Z (2016년 12월 5일 오전 4시 20분)인 경우 실제 종료 시간은 2016년 12월 5일 오전 5시 20분으로 설정됩니다. 특정 변경 유형에 ExpectedExecutionDurationInMinutes 대한를 찾으려면 다음 명령을 실행합니다.

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Note

실행 모드가 수동인 예약된 RFCs 콘솔에서 최소 24시간 후에 실행되도록 설정해야 합니다. 이 주의 사항은 AMS API/CLI에는 적용되지 않지만 최소 8시간 전에 수동 RFCs를 예약하는 것이 중요합니다.

Note

'검토 필요' CTs를 사용하는 경우 ASAP 예약 옵션(콘솔에서 ASAP 선택, API/CLI에서 시작 및 종료 시간 비워 두기)을 사용하는 것이 좋습니다. 이러한 CTs는 AMS 운영자가 RFC를 검사하고 승인 및 실행 전에 사용자와 통신해야 하기 때문입니다. 이러한 RFCs 예약하는 경우 최소 24시간을 허용해야 합니다. 예정된 시작 시간 전에 승인이 이루어지지 않으면 RFC가 자동으로 거부됩니다.

AMS는 4시간 이내에 수동 CT에 응답하는 것을 목표로 하며 가능한 한 빨리 대응하지만 RFC를 실제로 실행하는 데 훨씬 더 오래 걸릴 수 있습니다.

수동이고 AMS 검토가 필요한 CTs 목록은 콘솔의 개발자 리소스 페이지에서 사용할 수 있는 변경 유형 CSV 파일을 참조하세요.

YouTube 동영상: [AMS RFCs 하나요?](#)

AMS 콘솔에서 CT의 실행 모드를 찾으려면 변경 유형 찾아보기 검색 옵션을 사용해야 합니다. 결과는 일치하는 변경 유형 또는 변경 유형의 실행 모드를 보여줍니다.

AMS CLI를 사용하여 특정 변경 유형에 AutomationStatus 대한를 찾으려면 다음 명령을 실행합니다.

```
aws amscm --profile sam1 get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

모든 [AMS 변경 유형에 대한 정보를 제공하는 AMS 변경 유형 참조](#)에서 변경 유형을 조회할 수도 있습니다.

Note

AMS API/CLI는 현재 AWS API/CLI에 속하지 않습니다. AMS API/CLI에 액세스하려면 AMS 콘솔을 통해 AMS SDK를 다운로드합니다.

CT 승인 요구 사항

AMS CTs에는 항상 `AwsApprovalId`와 `CustomerApprovalId`라는 두 가지 승인 조건이 있으며, 이는 RFC가 실행을 승인하기 위해 AMS 또는 사용자 또는 다른 사람이 필요한지 여부를 나타냅니다.

승인 조건은 실행 모드와 다소 관련이 있습니다. 자세한 내용은 섹션을 참조하세요 [자동 및 수동 CTs](#).

CT의 승인 조건을 확인하려면 [AMS 변경 유형 참조](#)에서 확인하거나 [GetChangeTypeVersion](#)을 실행합니다. 둘 다 CT AutomationStatusId 또는 실행 모드도 제공합니다.

AMS 콘솔을 사용하거나 다음 명령을 사용하여 RFCs를 승인할 수 있습니다.

```
aws amscm approve-rfc --rfc-id RFC_ID
```

CT 승인 조건

CT 승인 조건이 인 경우	의 승인이 필요합니다.	및
<code>AwsApprovalId: Required</code>	AMS 변경 유형 시스템	아무 조치도 필요하지 않습니다. 이 조건은 자동 CTs의 경우 일반적입니다.
<code>AwsApprovalId: NotRequiredIfSubmitter</code>	제출된 RFC가 제출된 계정에 대한 경우 AMS 변경 유형 시스템이며 다른 사람은 없습니다.	아무 조치도 필요하지 않습니다. 이 조건은 AMS 운영자가 항상 검토하므로 수동 CTs의 경우 일반적입니다.

CT 승인 조건이 인 경우	의 승인이 필요 합니다.	및
CustomerApprovalId: NotRequired	AMS 변경 유형 시스템	RFC가 구문 및 파라미터 검사를 통과하 면 자동으로 승인됩니다.
CustomerApprovalId: Required	AMS 변경 유형 시스템 및 사용 자,	알림이 전송되므로 알림에 응답하거나 ApproveRfc 작업을 실행하여 RFC를 명시 적으로 승인해야 합니다.
CustomerApprovalId: NotRequiredIfSubmitter	RFC를 제출한 경우 AMS 변경 유형 시스템이 며 다른 사람은 없습니다.	RFC가 구문 및 파라미터 검사를 통과하 면 자동으로 승인됩니다.
긴급 보안 인시던트 또는 패치	AMS	자동 승인되고 구현됩니다.

유형 버전 변경

변경 유형은 버전이 지정되고 변경 유형에 대한 주요 업데이트가 수행되면 버전이 변경됩니다.

AMS 콘솔을 사용하여 변경 유형을 선택한 후 추가 구성 영역을 열고 변경 유형 버전을 선택할 수 있습니다. API/CLI 명령줄에서 변경 유형 버전을 지정할 수도 있습니다. 다음과 같은 다양한 이유로 작업을 수행할 수 있습니다.

- 원하는 업데이트 변경 유형의 버전은 현재 업데이트하려는 리소스를 생성하는 데 사용한 변경 생성 유형의 버전과 일치해야 합니다. 예를 들어 ELB 변경 유형 버전 1 생성을 사용하여 생성한 Elastic Load Balancer(ELB) 인스턴스가 있을 수 있습니다. 업데이트하려면 ELB 업데이트 버전 1을 선택합니다.
- 최신 변경 유형과 다른 옵션이 있는 변경 유형 버전을 사용하려고 합니다. AMS 업데이트는 주로 보안상의 이유로 유형을 변경하므로 권장하지 않으며 항상 최신 버전을 선택하는 것이 좋습니다.

변경 유형 생성

변경 유형 생성은 version-to-version 변경 유형 업데이트와 일치합니다. 즉, 리소스를 프로비저닝하는 데 사용하는 변경 유형 버전은 나중에 해당 리소스를 수정하는 데 사용할 업데이트 변경 유형 버전과 일치해야 합니다. 예를 들어 S3 버킷 변경 유형 생성 버전 2.0으로 S3 버킷을 생성하고 나중에 RFC를

제출하여 해당 S3 버킷을 수정하려는 경우 버전 S3.0으로 S3 버킷 업데이트 변경 유형이 있더라도 S3 버킷 업데이트 변경 유형 버전 2.0도 사용해야 합니다.

나중에 변경 유형 업데이트를 사용하여 수정하려는 경우 변경 유형 생성으로 리소스를 프로비저닝할 때 사용하는 변경 유형 ID 및 버전에 대한 레코드를 보관하는 것이 좋습니다.

변경 유형 업데이트

AMS는 변경 유형 생성을 사용하여 생성된 리소스를 업데이트하는 업데이트 변경 유형을 제공합니다. 업데이트 변경 유형은 원래 리소스를 프로비저닝하는 데 사용된 변경 생성 유형과 version-to-version 일치해야 합니다.

리소스를 쉽게 업데이트할 수 있도록 리소스를 프로비저닝할 때 사용하는 변경 유형 ID 및 버전을 기록해 두는 것이 좋습니다.

YouTube 동영상: [업데이트 CTs 사용하여 AWS Managed Services\(AMS\) 계정의 리소스를 변경하려면 어떻게 해야 하나요?](#)

내부 전용 변경 유형

내부 전용 변경 유형을 볼 수 있습니다. 따라서 AMS가 수행할 수 있거나 수행할 수 있는 작업을 알 수 있습니다. 사용하려는 내부 전용 변경 유형이 있는 경우 서비스 요청을 제출합니다.

예를 들어 내부 전용인 관리 | 모니터링 및 알림 | CloudWatch 경보 억제 | CT 업데이트가 있습니다. AMS는 이를 사용하여 인프라 업데이트(패칭 등)를 배포하고 업데이트가 잘못 트리거될 수 있는 경보 알림을 끕니다. 이 CT가 제출되면 RFC 목록에 CT의 RFC가 표시됩니다. RFC에 배포된 모든 내부 전용 CT는 RFC 목록에 표시됩니다.

변경 유형 스키마

모든 변경 유형은 리소스의 생성, 수정 또는 액세스 시 입력에 대한 JSON 스키마를 제공합니다. 스키마는 변경 요청(RFC)을 생성할 수 있도록 파라미터와 설명을 제공합니다.

RFC를 성공적으로 실행하면 실행 출력이 생성됩니다. RFCs 프로비저닝의 경우 실행 출력에는 CloudFormation의 스택을 나타내며 CloudFormation 콘솔에서 검색할 수 있는 "stack_id"가 포함됩니다. 실행 출력에는 생성된 인스턴스의 ID 출력이 포함되고 해당 ID를 사용하여 해당 AWS 콘솔에서 인스턴스를 검색할 수 있습니다. 예를 들어 ELB CT 실행 생성 출력에는 CloudFormation에서 검색할 수 있는 "stack_id"가 포함되며 Amazon EC2 콘솔에서 Elastic Load Balancing에 대해 검색할 수 있는 키=ELB 값=<stack-xxxx>가 출력됩니다.

CT 스키마를 살펴보겠습니다. 이것은 상당히 작은 스키마인 CodeDeploy Application Create의 스키마입니다. 일부 스키마에는 매우 큰 Parameter 영역이 있습니다.


```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv000000000000",
      "type": "string",
      "enum": ["stm-sft6rv000000000000"]
    },
    "Name": {
      "description": "A name for the stack or stack component
;
      this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
categorize the resource.",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "Key": {
            "type": "string",
            "minLength": 1,

```

스키마의 첫 번째 부분은 요청된 변경 유형에 대한 정보를 AMS에 제공합니다.

TimeoutInMinutes 파라미터를 사용하면 변경 유형을 실행하기 위

```

        "maxLength": 127
      },
      "Value": {
        "type": "string",
        "minLength": 1,
        "maxLength": 255
      }
    },
    "additionalProperties": false,
    "required": [
      "Key",
      "Value"
    ]
  },
  "minItems": 1,
  "maxItems": 7
},
"TimeoutInMinutes": {
  "description": "The maximum amount of time, in minutes,
to
  allow for execution of the change. This will not prolong
execution,
  but the RFC fails if the change is not completed in the
specified time.
  Valid values are 60 up to 360, for long-running
UserData.",
  "type": "number",
  "minimum": 0,
  "maximum": 60
},
"Parameters": {
  "description": "Specifications for the stack.",
  "type": "object",
  "properties": {
    "CodeDeployApplicationName": {
      "description": "The name of an AWS CodeDeploy
application.",
      "type": "string",
      "minLength": 1,
      "maxLength": 100,
      "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
    }
  }
},
"additionalProperties": false,

```

한 경계 시간을 표시할 수 있습니다. 장기 실행 UserData의 경우 유효한 값은 60~360입니다.

파라미터 섹션에서는 생성 중인 리소스 또는 요청 중인 작업에 대한 설정을 지정합니다.

"추가 속성" 섹션에서는 필요한 파라미터와 선택 사항인 파라미터를 알 수 있습니다.

```

    "required": [
      "CodeDeployApplicationName"
    ]
  },
  "additionalProperties": false,
  "required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
  ]
}

```

Note

이 스키마는 최대 7개의 태그를 허용하지만 EC2, EFS, RDS 및 다중 계층 생성 스키마는 최대 50개의 태그를 허용합니다.

변경 유형에 대한 권한 관리

사용자 지정 정책을 사용하여 다른 그룹 또는 사용자가 사용할 수 있는 변경 유형(CTs)을 제한할 수 있습니다.

이에 대한 자세한 내용은 AMS 사용 설명서의 [권한 설정을 참조하세요](#).

변경 유형에서 민감한 정보 수정

AMS 변경 유형 스키마 "metadata": "ams:sensitive": "true"는 암호와 같은 민감한 정보를 포함하는 파라미터에 사용되는 파라미터 속성을 제공합니다. 이 속성을 설정하면 제공된 입력이 가려집니다. 이 파라미터 속성은 설정할 수 없지만 AMS를 사용하여 변경 유형을 생성하고 입력 시 가려야 하는 파라미터가 있는 경우 이를 요청할 수 있습니다.

쿼리 옵션을 사용하여 변경 유형 찾기

이 예제에서는 AMS 콘솔을 사용하여 제출하려는 RFC에 적합한 변경 유형을 찾는 방법을 보여줍니다.

콘솔 또는 API/CLI를 사용하여 변경 유형 ID(CT) 또는 버전을 찾을 수 있습니다. 검색 또는 분류 선택이라는 두 가지 방법이 있습니다. 두 선택 유형 모두 가장 자주 사용, 가장 최근에 사용 또는 알파벳순을 선택하여 검색을 정렬할 수 있습니다.

YouTube 동영상: [AWS Managed Services CLI를 사용하여 RFC를 생성하려면 어떻게 해야 하고 CT 스키마는 어디에서 찾을 수 있습니까?](#)

AMS 콘솔의 RFCs

- 변경 유형별 찾아보기(기본값)를 선택한 상태에서 다음 중 하나를 수행합니다.
 - 빠른 생성 영역을 사용하여 AMS의 가장 인기 CTs 중에서 선택합니다. 레이블을 클릭하면 제목 옵션이 자동으로 채워진 RFC 실행 페이지가 열립니다. 필요에 따라 나머지 옵션을 완료하고 실행을 클릭하여 RFC를 제출합니다.
 - 또는 모든 변경 유형 영역까지 아래로 스크롤하여 옵션 상자에 CT 이름을 입력하기 시작합니다. 정확한 변경 유형 이름이나 전체 변경 유형 이름을 가질 필요는 없습니다. 관련 단어를 입력하여 변경 유형 ID, 분류 또는 실행 모드(자동 또는 수동)별로 CT를 검색할 수도 있습니다.

기본 카드 보기를 선택하면 입력 시 일치하는 CT 카드가 나타나고 카드를 선택한 다음 RFC 생성을 클릭합니다. 테이블 보기를 선택한 상태에서 관련 CT를 선택하고 RFC 생성을 클릭합니다. 두 방법 모두 RFC 실행 페이지를 엽니다.

- 또는 변경 유형 선택을 탐색하려면 페이지 상단의 범주별 선택을 클릭하여 일련의 드롭다운 옵션 상자를 엽니다.
- 범주, 하위 범주, 항목 및 작업을 선택합니다. 해당 변경 유형에 대한 정보 상자가 페이지 하단에 패널이 나타납니다.
- 준비가 되면 Enter 키를 누르면 일치하는 변경 유형 목록이 나타납니다.
- 목록에서 변경 유형을 선택합니다. 해당 변경 유형에 대한 정보 상자가 페이지 하단에 나타납니다.
- 올바른 변경 유형을 지정한 후 RFC 생성을 선택합니다.

Note

이러한 명령이 작동하려면 AMS CLI가 설치되어 있어야 합니다. AMS API 또는 CLI를 설치하려면 AMS 콘솔 개발자 리소스 페이지로 이동합니다. AMS CM API 또는 AMS SKMS API에 대한 참조 자료는 사용 설명서의 AMS 정보 리소스 섹션을 참조하세요. 인증 `--profile` 옵션을 추가해야 할 수 있습니다. 예: `aws amsskms ams-cli-command --profile SAML`. 와 같이 모든 AMS 명령이 `us-east-1`에서 부족하므로 `--region` 옵션을 추가해야 할 수도 있습니다. `aws amscm ams-cli-command --region=us-east-1`.

Note

AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다us-east-1. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 --region us-east-1 때를 추가해야 할 수 있습니다. 인증 방법인 --profile saml 경우를 추가해야 할 수도 있습니다.

AMS CM API([ListChangeTypeClassificationSummaries](#) 참조) 또는 CLI를 사용하여 변경 유형을 검색하려면

필터 또는 쿼리를 사용하여 검색할 수 있습니다. ListChangeTypeClassificationSummaries 작업에는 Category, SubcategoryItem, 및에 대한 [필터](#) 옵션이 0operation있지만 값은 기존 값과 정확히 일치해야 합니다. CLI를 사용할 때 보다 유연한 결과를 얻으려면 --query 옵션을 사용할 수 있습니다.

AMS CM API/CLI를 사용한 유형 필터링 변경

속성	유효값	유효/기본 조건	참고
ChangeTypeId	ChangeTypeId를 나타내는 모든 문자열(예: ct-abc123xyz7890)	같음	변경 유형 IDs는 변경 유형 참조 를 참조하세요. 변경 유형 IDs는 변경 유형 찾기 또는 CSIO를 참조하세요.
범주	모든 자유 형식 텍스트	포함	각 개별 필드의 정규식은 지원되지 않습니다. 대/소문자를 구분하지 않는 검색
Subcategory			
Item			
연산			

1. 다음은 변경 유형 분류를 나열하는 몇 가지 예입니다.

다음 명령은 모든 변경 유형 범주를 나열합니다.

```
aws amscm list-change-type-categories
```

다음 명령은 지정된 범주에 속하는 하위 범주를 나열합니다.

```
aws amscm list-change-type-subcategories --category CATEGORY
```

다음 명령은 지정된 범주 및 하위 범주에 속하는 항목을 나열합니다.

```
aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
```

2. 다음은 CLI 쿼리를 사용하여 변경 유형을 검색하는 몇 가지 예입니다.

다음 명령은 항목 이름에 "S3"가 포함된 CT 분류 요약을 검색하고 범주, 하위 범주, 항목, 작업 및 변경 유형 ID의 출력을 테이블 형식으로 생성합니다.

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-----+-----+-----+-----+-----+
|               ListChangeTypeClassificationSummaries               |
+-----+-----+-----+-----+-----+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+-----+-----+-----+-----+-----+
```

3. 그런 다음 변경 유형 ID를 사용하여 CT 스키마를 가져오고 파라미터를 검사할 수 있습니다. 다음 명령은 스키마를 CreateS3Params.schema.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
  --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
  CreateS3Params.schema.json
```

CLI 쿼리 사용에 대한 자세한 내용은 [--query 옵션을 사용하여 출력을 필터링하는 방법](#) 및 쿼리 언어 참조인 [JMESPath 사양](#)을 참조하세요.

4. 변경 유형 ID가 있으면 변경 유형의 버전을 확인하여 최신 버전인지 확인하는 것이 좋습니다. 이 명령을 사용하여 지정된 변경 유형의 버전을 찾습니다.

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

특정 변경 유형에 AutomationStatus 대한를 찾으려면 다음 명령을 실행합니다.

```
aws amscm --profile sam1 get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

특정 변경 유형에 ExpectedExecutionDurationInMinutes 대한를 찾으려면 다음 명령을 실행합니다.

```
aws amscm --profile sam1 get-change-type-version --change-type-id ct-14027q0sjyt1h
--query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

AMS의 RFC 오류 문제 해결

CloudFormation 설명서를 통해 많은 AMS 프로비저닝 RFC 실패를 조사할 수 있습니다. [AWS CloudFormation 문제 해결: 오류 문제 해결을 참조하세요.](#)

추가 문제 해결 제안은 다음 섹션에 나와 있습니다.

AMS의 “관리” RFC 오류

AMS "관리" 범주 변경 유형(CTs)을 사용하면 리소스에 대한 액세스를 요청하고 기존 리소스를 관리할 수 있습니다. 이 섹션에서는 몇 가지 일반적인 문제를 설명합니다.

RFC 액세스 오류

- RFC에 지정한 사용자 이름과 FQDN이 올바르고 도메인에 존재하는지 확인합니다. FQDN을 찾는 데 도움이 필요하면 [FQDN 찾기를 참조하세요.](#)
- 액세스를 위해 지정한 스택 ID가 EC2-related 스택인지 확인합니다. ELB 및 Amazon Simple Storage Service(S3)와 같은 스택은 액세스 RFCs의 대상이 아니며, 대신 읽기 전용 액세스 역할을 사용하여 이러한 스택 리소스에 액세스합니다. 스택 ID 찾기에 대한 도움말은 [스택 IDs](#).
- 제공한 스택 ID가 올바르고 관련 계정에 속하는지 확인합니다.

다른 액세스 RFC 실패에 대한 도움말은 [액세스 관리를 참조하세요.](#)

YouTube 동영상: [거부 및 실패를 방지하기 위해 변경 요청\(RFC\)을 올바르게 제기하려면 어떻게 해야 하나요?](#)

RFC(수동) CT 예약 오류

대부분의 변경 유형은 ExecutionMode=Automated이지만 일부는 ExecutionMode=Manual이며 RFC 실패를 방지하기 위해 변경 유형을 예약하는 방법에 영향을 미칩니다.

ExecutionMode=ManualRFCs는 AMS 콘솔을 사용하여 RFC를 생성하는 경우 향후 최소 24시간 동안 실행되도록 설정해야 합니다. 이 주의 사항은 AMS API/CLI에는 적용되지 않지만 최소 8시간 전에 수동 RFCs를 예약하는 것이 중요합니다.

AMS는 4시간 이내에 수동 CT에 응답하는 것을 목표로 하며 가능한 한 빨리 대응하지만 RFC가 실제로 실행되는 데 훨씬 더 오래 걸릴 수 있습니다.

수동 업데이트 CTsRFCs 사용

업데이트하려는 스택 유형에 대한 업데이트 변경 유형이 있는 경우 AMS 작업은 스택 업데이트에 대한 관리 | 기타 | 기타 RFCs를 거부합니다.

RFC 스택 삭제 오류

RFC 스택 삭제 실패: 관리 | 표준 스택 | 스택 | CT 삭제를 사용하는 경우 AMS 스택 이름을 사용하여 스택에 대한 자세한 이벤트가 AWS CloudFormation 콘솔에 표시됩니다. AMS 콘솔에 있는 이름과 비교하여 스택을 식별할 수 있습니다. AWS CloudFormation 콘솔은 장애 원인에 대한 자세한 내용을 제공합니다.

스택을 삭제하기 전에 스택이 생성된 방법을 고려해야 합니다. AMS CT를 사용하여 스택을 생성하고 스택 리소스를 추가하거나 편집하지 않은 경우 문제 없이 스택을 삭제할 수 있습니다. 그러나 스택에 대해 스택 RFC 삭제를 제출하기 전에 스택에서 수동으로 추가된 리소스를 제거하는 것이 좋습니다. 예를 들어 전체 스택 CT(HA 2 티어)를 사용하여 스택을 생성하는 경우 보안 그룹 - SG1이 포함됩니다. 그런 다음 AMS를 사용하여 다른 보안 그룹 SG2를 생성하고 전체 스택의 일부로 생성된 SG1에서 새 SG2를 참조한 다음 스택 삭제 CT를 사용하여 스택을 삭제하면 SG2에서 참조하므로 SG1이 삭제되지 않습니다. SG2

Important

스택을 삭제하면 원치 않고 예상치 못한 결과가 발생할 수 있습니다. AMS는 이러한 이유로 고객을 대신하여 스택 또는 스택 리소스를 삭제*하지 않는 것을 선호합니다. AMS는 삭제하려는 적절한 자동 변경 유형을 사용하여 삭제할 수 없는 사용자 대신(제출된 관리 | 기타 | 기타 | 변경 유형 업데이트) 리소스만 삭제합니다. 추가 고려 사항:

- 리소스가 '삭제 방지'에 대해 활성화된 경우 AMS는 관리 | 기타 | 기타 | 변경 유형 업데이트를 제출하고 삭제 방지가 제거된 후 자동 CT를 사용하여 해당 리소스를 삭제할 경우 이를 차단 해제하는 데 도움이 될 수 있습니다.
- 스택에 여러 리소스가 있고 스택 리소스의 하위 집합만 삭제하려는 경우 CloudFormation 업데이트 변경 유형을 사용합니다([CloudFormation 수집 스택: 업데이트](#) 참조). 관리 | 기타 | 기타 | 변경 유형 업데이트도 제출할 수 있으며 필요한 경우 AMS 엔지니어가 변경 세트를 만드는 데 도움을 줄 수 있습니다.
- 드리프트로 인해 CloudFormation Update CT를 사용하는 데 문제가 있는 경우 관리 | 기타 | 기타 | 업데이트를 제출하여 드리프트를 해결하고(AWS CloudFormation Service에서 지원하는 범위까지) 자동 CT, CloudFormation 템플릿에서 관리/사용자 지정 스택/스택/변경 세트 승인 및 업데이트를 사용하여 검증하고 실행할 수 있는 ChangeSet를 제공하면 AMS가 도움이 될 수 있습니다. CloudFormation

AMS는 예상치 못하거나 예상치 못한 리소스 삭제가 없도록 위의 제한을 유지합니다.

자세한 내용은 [AWS CloudFormation 문제 해결: 스택 삭제 실패를 참조하세요](#).

RFC 업데이트 DNS 오류

DNS 호스팅 영역을 업데이트하는 여러 RFCs가 실패할 수 있으며, 일부 RFC는 이유 없이 실패할 수 있습니다. DNS 호스팅 영역(프라이빗 또는 퍼블릭)을 업데이트하기 위해 여러 RFCs를 동시에 생성하면 동일한 스택을 동시에 업데이트하려고 하기 때문에 일부 RFCs가 실패할 수 있습니다. AMS 변경 관리의 스택이 이미 다른 RFCs에 의해 업데이트되고 있기 때문에 스택을 업데이트할 수 없는 RFC를 거부하거나 실패합니다. AMS에서는 한 번에 하나의 RFC를 생성하고 RFC가 성공할 때까지 기다린 후 동일한 스택에 대해 새 RFC를 생성하는 것이 좋습니다.

RFC IAM 엔터티 오류

AMS는 요구 사항에 맞게 설계된 AMS 계정에 여러 기본 IAM 역할 및 프로필을 프로비저닝합니다. 그러나 가끔 추가 IAM 리소스를 요청해야 할 수 있습니다.

사용자 지정 IAM 리소스를 요청하는 RFCs를 제출하는 프로세스는 수동 RFCs의 표준 워크플로를 따르지만 승인 프로세스에는 적절한 보안 제어가 마련되어 있는지 확인하기 위한 보안 검토도 포함됩니다. 따라서 프로세스는 일반적으로 다른 수동 RFCs보다 오래 걸립니다. 이러한 RFCs의 주기 시간을 줄이려면 다음 지침을 따르세요.

IAM 검토의 의미와 기술 표준 및 위험 수락 프로세스에 매핑되는 방법에 대한 자세한 내용은 섹션을 참조하세요 [RFC 보안 검토 이해](#).

일반적인 IAM 리소스 요청:

- CloudEndure와 같은 주요 클라우드 호환 애플리케이션과 관련된 정책을 요청하는 경우 AMS 사전 승인된 IAM CloudEndure 정책: [WIGs Cloud Endure Landing Zone 예제](#) 파일의 압축을 풀고 customer_cloud_endure_policy.json

Note

보다 허용적인 정책을 원하는 경우 CloudArchitect/CSDM과 요구 사항에 대해 논의하고 필요한 경우 정책을 구현하는 RFC를 제출하기 전에 AMS 보안 검토 및 승인을 받습니다.

- 기본적으로 계정의 AMS에서 배포한 리소스를 수정하려면 기존 리소스를 변경하는 대신 해당 리소스의 수정된 사본을 요청하는 것이 좋습니다.
- 인간 사용자에게 권한을 요청하는 경우(사용자에게 권한을 연결하는 대신) 역할에 권한을 연결한 다음 사용자에게 해당 역할을 수임할 수 있는 권한을 부여합니다. 이에 대한 자세한 내용은 [임시 AMS 고급 콘솔 액세스](#)를 참조하세요.
- 임시 마이그레이션 또는 워크플로에 대한 예외적인 권한이 필요한 경우 요청에서 해당 권한의 종료 날짜를 제공합니다.
- 요청의 주체에 대해 보안 팀과 이미 논의한 경우 CSDM에 승인 증거를 최대한 자세히 제공합니다.

AMS가 IAM RFC를 거부하는 경우 거부에 대한 명확한 이유를 제공합니다. 예를 들어 IAM 정책 생성 요청을 거부하고 정책에 대한 부적절한 내용을 설명할 수 있습니다. 이 경우 식별된 변경을 수행하고 요청을 다시 제출할 수 있습니다. 요청 상태에 대한 추가 설명이 필요한 경우 서비스 요청을 제출하거나 CSDM에 문의하십시오.

다음 목록은 IAM RFCs를 검토할 때 AMS가 완화하려고 하는 일반적인 위험을 설명합니다. IAM RFC에 이러한 위험이 있는 경우 RFC가 거부될 수 있습니다. 예외가 필요한 경우 AMS는 보안 팀에 승인을 요청합니다. 이러한 예외를 찾으려면 CSDM과 조정하십시오.

Note

AMS는 어떤 이유로든 계정 내 IAM 리소스에 대한 변경을 거부할 수 있습니다. RFC 거부와 관련된 우려 사항은 서비스 요청을 통해 AMS Operations에 문의하거나 CSDM에 문의하십시오.

- 자체 권한을 수정하거나 계정 내 다른 리소스의 권한을 수정할 수 있는 권한과 같은 권한 에스컬레이션. 예시:
 - 더 많은 권한을 가진 다른 역할과 `iam:PassRole` 함께를 사용합니다.
 - 역할 또는 사용자로부터 IAM 정책을 연결/분리할 수 있는 권한.
 - 계정의 IAM 정책 수정.
 - 관리 인프라의 맥락에서 API를 호출하는 기능입니다.
 - AMS 서비스를 제공하는 데 필요한 리소스 또는 애플리케이션을 수정할 수 있는 권한. 예시:
 - 접속, 관리 호스트 또는 EPS 인프라와 같은 AMS 인프라 수정.
 - 로그 관리 AWS Lambda 함수 또는 로그 스트림 삭제.
 - 기본 CloudTrail 모니터링 애플리케이션의 삭제 또는 수정입니다.
 - 디렉터리 서비스 Active Directory(AD)의 수정입니다.
 - CloudWatch(CW) 경보를 비활성화합니다.
 - 랜딩 존의 일부로 계정에 배포된 보안 주체, 정책 및 네임스페이스의 수정입니다.
 - 정보 보안을 위협하게 하는 상태에서 인프라를 생성할 수 있는 권한과 같은 모범 사례를 벗어나는 인프라 배포. 예시:
 - 퍼블릭 또는 암호화되지 않은 S3 버킷 생성 또는 EBS 볼륨의 퍼블릭 공유.
 - 퍼블릭 IP 주소의 프로비저닝입니다.
 - 광범위한 액세스를 허용하도록 보안 그룹을 수정했습니다.
 - 인프라 및 계정 내 애플리케이션에 대한 데이터 손실, 무결성 손실, 부적절한 구성 또는 서비스 중단을 초래할 수 있는 권한과 같이 애플리케이션에 영향을 미칠 수 있는 지나치게 광범위한 권한. 예시:
 - `ModifyNetworkInterfaceAttribute` 또는와 같은 APIs를 통해 네트워크 트래픽을 비활성화하거나 리디렉션합니다UpdateRouteTable.
 - 관리형 호스트에서 볼륨을 분리하여 관리형 인프라를 비활성화합니다.
 - AMS 서비스 설명의 일부가 아니며 AMS에서 지원하지 않는 서비스에 대한 권한.
- AMS 서비스 설명에 나열되지 않은 서비스는 AMS 계정에서 사용할 수 없습니다. 기능 또는 서비스에 대한 지원을 요청하려면 CSDM에 문의하십시오.
- 너무 관대하거나 보수적이거나 잘못된 리소스에 적용되므로 명시된 목표를 충족하지 않는 권한. 예시:
 - 관련 키에 대한 `s3:PutObject` 권한 없이 필수 KMS 암호화가 있는 S3 버킷에 대한 `KMS:Encrypt` 권한 요청입니다.

- RFCs의 설명이 요청과 일치하지 않는 것으로 보이는 IAM RFC입니다.

“배포” RFC 오류

AMS "배포" 범주 변경 유형(CTs)을 사용하면 다양한 AMS 지원 리소스를 계정에 추가하도록 요청할 수 있습니다.

리소스를 생성하는 대부분의 AMS CTs는 AWS CloudFormation 템플릿을 기반으로 합니다. 고객은 AWS CloudFormation 콘솔을 사용하여 AWS CloudFormation 스택 설명을 기반으로 스택을 나타내는 스택을 빠르게 식별할 AWS CloudFormation 수 있습니다. 실패한 스택은 DELETE_COMPLETE 상태 일 수 있습니다. AWS CloudFormation 스택을 식별하면 이벤트에 생성에 실패한 특정 리소스와 이유가 표시됩니다.

CloudFormation 설명서를 사용하여 문제 해결

대부분의 AMS 프로비저닝 RFCs는 CloudFormation 템플릿을 사용하며 설명서는 문제 해결에 유용할 수 있습니다. 해당 AWS CloudFormation 템플릿에 대한 설명서를 참조하세요.

- 애플리케이션 로드 밸런서 생성 실패: [AWS::ElasticLoadBalancingV2::LoadBalancer\(Application Load Balancer\)](#)
- Auto Scaling 그룹 생성: [AWS::AutoScaling::AutoScalingGroup\(Auto Scaling 그룹\)](#)
- memcached 캐시 생성: [AWS::ElastiCache::CacheCluster\(캐시 클러스터\)](#)
- Redis 캐시 생성: [AWS::ElastiCache::CacheCluster\(캐시 클러스터\)](#)
- DNS 호스팅 영역 생성(DNS 프라이빗/퍼블릭 생성과 함께 사용): [AWS::Route53::HostedZone\(R53 호스팅 영역\)](#)
- DNS 레코드 세트 생성(DNS 프라이빗/퍼블릭 생성과 함께 사용): [AWS::Route53::RecordSet\(리소스 레코드 세트\)](#)
- EC2 스택 생성: [AWS::EC2::Instance\(Elastic Compute Cloud\)](#)
- EFS(Elastic File System): [AWS::EFS::FileSystem\(Elastic File System\)](#)
- 로드 밸런서 생성: [AWS::ElasticLoadBalancing::LoadBalancer\(Elastic Load Balancer\)](#)
- RDS DB 생성: [AWS::RDS::DBInstance\(관계형 데이터베이스\)](#)
- Amazon S3 생성: [AWS::S3::Bucket\(Simple Storage Service\)](#)
- 대기열 생성: [AWS::SQS::Queue\(단순 대기열 서비스\)](#)

RFC 생성 AMIs 오류

Amazon Machine Image(AMI)는 소프트웨어 구성이 기재된 템플릿입니다(예: 운영 체제, 애플리케이션 서버, 애플리케이션). AMI에서 인스턴스를 바로 시작할 수 있는데, 이 인스턴스는 AMI의 사본으로, 클라우드에서 실행되는 가상 서버입니다. AMIs는 매우 유용하며 EC2 인스턴스 또는 Auto Scaling 그룹을 생성하는 데 필요하지만 몇 가지 요구 사항을 준수해야 합니다.

- RFC가 성공하려면에 대해 지정하는 인스턴스가 중지 상태여야 Ec2InstanceId 합니다. ASG가 중지된 인스턴스를 종료하므로이 파라미터에 Auto Scaling 그룹(ASG) 인스턴스를 사용하지 마십시오.
- AMS Amazon Machine Image(AMI)를 생성하려면 AMS 인스턴스로 시작해야 합니다. 인스턴스를 사용하여 AMI를 생성하려면 먼저 인스턴스가 중지되고 도메인에서 조인 해제되었는지 확인하여 인스턴스를 준비해야 합니다. 자세한 내용은 [Sysprep을 사용하여 표준 Amazon Machine Image 생성](#)을 참조하세요.
- 새 AMI에 지정하는 이름은 계정 내에서 고유해야 합니다. 그렇지 않으면 RFC가 실패합니다. 이 작업을 수행하는 방법은 [AMI | 생성](#)에 설명되어 있으며, 자세한 내용은 및 [AWS AMI 설계를](#) 참조하세요.

Note

AMI 생성 준비에 대한 자세한 내용은 [AMI | 생성](#)을 참조하세요.

EC2s 또는 ASGs 오류를 생성하는 RFCs

제한 시간이 있는 EC2 또는 ASG 실패의 경우 AMS는 사용된 AMI가 사용자 지정되었는지 확인할 것을 권장합니다. 그렇다면이 가이드에 포함된 AMI 생성 단계([AMI | 생성](#) 참조)를 참조하여 AMI가 올바르게 생성되었는지 확인하세요. 사용자 지정 AMI를 생성할 때 흔히 발생하는 실수는 가이드의 단계를 따라 Sysprep의 이름을 바꾸거나 호출하는 것이 아닙니다.

RDS 오류를 생성하는 RFCs

Amazon Relational Database Service(RDS) 장애는 RDS를 생성할 때 다양한 엔진을 사용할 수 있으며 각 엔진에는 고유한 요구 사항과 제한이 있기 때문에 여러 가지 이유로 발생할 수 있습니다. AMS RDS 스택을 생성하기 전에 AWS RDS 파라미터 값을 주의 깊게 검토하세요. [CreateDBInstance](#)를 참조하세요.

크기 권장 사항을 포함하여 일반적으로 Amazon RDS에 대한 자세한 내용은 [Amazon Relational Database Service 설명서](#)를 참조하세요.

Amazon S3s 오류를 생성하는 RFCs

S3 스토리지 버킷을 생성할 때 발생하는 한 가지 일반적인 오류는 버킷에 고유한 이름을 사용하지 않는 것입니다. 이전에 제출한 것과 동일한 이름의 S3 버킷 CT 생성을 제출한 경우 해당 BucketName에 S3 버킷이 이미 존재하기 때문에 실패합니다. 이는 AWS CloudFormation 스택 이벤트에서 버킷 이름이 이미 사용 중임을 보여주는 콘솔에 자세히 설명되어 있습니다.

RFC 검증과 실행 오류 비교

RFC 실패 및 관련 메시지는 선택한 RFC에 대한 AMS 콘솔 RFC 세부 정보 페이지의 출력 메시지에서 다릅니다.

- 검증 실패 이유는 상태 필드에서만 사용할 수 있습니다.
- 실행 실패 이유는 실행 출력과 상태 필드에서 확인할 수 있습니다.

RFC 오류 메시지

나열된 변경 유형(CTs)에 대해 다음 오류가 발생하면 이러한 솔루션을 사용하여 문제의 원인을 찾고 수정할 수 있습니다.

```
{"errorMessage":"An error has occurred during RFC execution. We are investigating the issue.", "errorType":"InternalError"}
```

다음 문제 해결 옵션을 참조한 후 추가 지원이 필요한 경우 RFC 서신을 통해 AMS를 참여시키거나 서비스 요청을 생성합니다. 자세한 내용은 [RFC 서신 및 연결\(콘솔\)](#) 및 [AMS에서 서비스 요청 생성](#)을 참조하세요.

워크로드 수집(WIGS) 오류

Note

Windows 및 Linux용 검증 도구를 다운로드하여 온프레미스 서버와 AWS의 EC2 인스턴스에서 직접 실행할 수 있습니다. AMS 고급 애플리케이션 개발자 안내서 [워크로드 마이그레이션: Linux 사전 수집 검증](#) 및 [워크로드 마이그레이션: Windows 사전 수집 검증](#)을 통해 확인할 수 있습니다.

- EC2 인스턴스가 대상 AMS 계정에 있는지 확인합니다. 예를 들어 비 AMS 계정에서 AMS 계정으로 AMI를 공유한 경우 워크로드 수집 RFC를 제출하기 전에 공유 AMI를 사용하여 AMS 계정에 EC2 인스턴스를 생성해야 합니다.
- 인스턴스에 연결된 보안 그룹에 송신 트래픽이 허용되는지 확인합니다. SSM 에이전트는 퍼블릭 엔드포인트에 연결할 수 있어야 합니다.
- 인스턴스에 SSM 에이전트와 연결할 수 있는 적절한 권한이 있는지 확인합니다. 이러한 권한은와 함께 제공되며 EC2 콘솔에서 이를 확인할 `customer-mc-ec2-instance-profile` 수 있습니다.

EC2 인스턴스 스택 중지 오류

- 인스턴스가 이미 중지되거나 종료된 상태인지 확인합니다.
- EC2 인스턴스가 온라인 상태이고 `InternalError` 오류가 표시되면 AMS가 조사할 서비스 요청을 제출합니다.
- 변경 유형 관리 | 고급 스택 구성 요소 | EC2 인스턴스 스택 | `ct-3mvt2zkyveqj` 중지를 사용하여 Auto Scaling 그룹(ASG) 인스턴스를 중지할 수 없습니다. ASG 인스턴스를 중지해야 하는 경우 서비스 요청을 제출합니다.

EC2 인스턴스 스택 생성 오류

메시지는 `CREATION_FAILED` 상태 이유인 CloudFormation에서 보낸 `InternalError` 것입니다. 다음 단계에 따라 CloudWatch 스택 이벤트의 스택 실패에 대한 세부 정보를 찾을 수 있습니다.

- AWS Management 콘솔에서 스택이 생성, 업데이트 또는 삭제되는 동안 스택 이벤트 목록을 볼 수 있습니다. 이 목록에서 실패 이벤트를 찾은 다음 해당 이벤트에 대한 상태 사유를 확인할 수 있습니다.

상태 이유에는 문제를 이해하는 데 도움이 될 수 있는 AWS CloudFormation 또는 특정 서비스의 오류 메시지가 포함될 수 있습니다.

- 스택 이벤트 보기에 대한 자세한 내용은 [AWS Management Console에서 AWS CloudFormation 스택 데이터 및 리소스 보기를 참조하세요](#).

EC2 인스턴스 볼륨 복원 오류

AMS는 EC2 인스턴스 볼륨 복원에 실패할 때 내부 문제 해결 RFC를 생성합니다. 이는 EC2 인스턴스 볼륨 복원이 재해 복구(DR)의 중요한 부분이며 AMS가 내부 문제 해결 RFC를 자동으로 생성하기 때문입니다.

내부 문제 해결 RFC가 생성되면 RFC에 대한 링크를 제공하는 배너가 표시됩니다. 이 내부 문제 해결 RFC에는 RFC 장애에 대한 더 많은 가시성을 제공하며, 동일한 오류로 이어지는 재시도 RFCs를 제출하거나 장애에 대해 AMS에 수동으로 연락하는 대신 변경 사항을 추적하고 AMS에서 장애를 처리하고 있음을 알 수 있습니다. 또한 AMS 운영자가 요청을 기다리는 대신 RFC 장애에 대해 사전에 작업하므로 변경 사항에 대한 TTR(time-to-recovery) 지표가 줄어듭니다.

RFC에 대한 도움을 받는 방법

AMS에 문의하여 실패의 근본 원인을 식별할 수 있습니다. AMS 업무 시간은 하루 24시간, 주 7일, 1년 365일입니다.

AMS는 도움을 요청하거나 서비스 요청을 할 수 있는 몇 가지 방법을 제공합니다.

- 정보나 조언을 요청하거나 AMS 관리형 IT 서비스에 액세스하거나 AMS에서 추가 서비스를 요청하려면 AMS 콘솔을 사용하여 서비스 요청을 제출합니다. 자세한 내용은 [서비스 요청 생성을 참조하세요](#). AMS 서비스 요청에 대한 일반 정보는 [서비스 요청 관리](#)를 참조하세요.
- 관리형 환경에 영향을 미치는 AWS 또는 AMS 서비스 성능 문제를 보고하려면 AMS 콘솔을 사용하여 인시던트 보고서를 제출합니다. 자세한 내용은 [인시던트 보고를 참조하세요](#). AMS 인시던트 관리에 대한 일반적인 정보는 [인시던트 대응](#)을 참조하세요.
- 사용자 또는 리소스 또는 애플리케이션이 AMS로 작업하는 방식에 대한 구체적인 질문이 있거나 인시던트를 에스컬레이션하려면 다음 중 하나 이상을 이메일로 보내십시오.
 1. 먼저 서비스 요청 또는 인시던트 보고서 응답이 만족스럽지 않은 경우 CSDM에 ams-csdm@amazon.com으로 이메일을 보냅니다.
 2. 다음으로 에스컬레이션이 필요한 경우 AMS Operations Manager에 이메일을 보낼 수 있습니다 (하지만 CSDM에서 작업을 수행할 수 있음). ams-opsmanager@amazon.com
 3. 추가 에스컬레이션은 AMS Director에게: ams-director@amazon.com
 4. 마지막으로 언제든지 AMS VP: ams-vp@amazon.com에 연결할 수 있습니다.

AMS의 직접 변경 모드

주제

- [직접 변경 모드 시작하기](#)
- [보안 및 규정 준수](#)
- [직접 변경 모드에서 변경 관리](#)
- [Direct Change 모드를 사용하여 스택 생성](#)
- [직접 변경 모드 사용 사례](#)

AWS Managed Services(AMS) Direct Change 모드(DCM)는 AMS Advanced Plus 및 Premium 계정에 대한 기본 AWS 액세스를 제공하여 AWS 리소스를 프로비저닝하고 업데이트함으로써 AMS Advanced 변경 관리를 확장합니다. DCM을 사용하면 네이티브 AWS API(콘솔 또는 CLI/SDK) 또는 AMS Advanced 변경 관리 요청(RFCs)을 사용할 수 있으며, 두 경우 모두 모니터링, 패치, 백업, 인시던트 대응 관리를 포함하여 AMS에서 리소스 및 변경 사항을 완전히 지원합니다. DCM을 통해 프로비저닝된 리소스는 AMS 서비스 지식 관리 시스템(SKMS)에 등록되고, AMS 관리형 Active Directory 도메인(해당하는 경우)에 조인되며, AMS 관리 에이전트를 실행합니다. 기존 도구(예: CloudFormation, AWS SDK 및 CDK)를 사용하여 AMS 관리형 CloudFormation 스택을 개발하고 배포합니다.

Note

직접 변경 모드는 AMS 변경 관리 RFCs 제거하지 않습니다. DCM을 사용하여 AMS RFCs 대한 전체 액세스 권한을 가집니다.

[Akash의 동영상을 보고 자세히 알아보기\(6:30\)](#)

직접 변경 모드 시작하기

먼저 사전 조건을 확인한 다음 적격 AMS Advanced 계정에서 변경 요청(RFC)을 제출합니다.

1. DCM과 함께 사용하려는 계정이 요구 사항을 충족하는지 확인합니다.
 - 계정은 AMS Advanced Plus 또는 Premium입니다.
 - 계정에 Service Catalog가 활성화되어 있지 않습니다. 현재 DCM과 Service Catalog 모두에 동시에 계정을 온보딩하는 것은 지원하지 않습니다. 이미 Service Catalog에 온보딩되어 있지만 DCM에 관심이 있는 경우 클라우드 서비스 제공 관리자(CSDM)와 요구 사항에 대해 논의하세요. Service Catalog에서 DCM으로 전환하기로 결정한 경우 Service Catalog를 오프보드하여 이를 수행하려면 아래 변경 요청에 요청을 포함하세요. AMS의 Service Catalog에 대한 자세한 내용은 [AMS 및 Service Catalog](#)를 참조하세요.

2. 관리 | 관리형 계정 | 직접 변경 모드 | 변경 유형 활성화(ct-3rd4781c2nnhp)를 사용하여 변경 요청(RFC)을 제출합니다. 예제 연습은 [직접 변경 모드 | 활성화](#)를 참조하세요.

CT가 처리되면 미리 정의된 IAM 역할 `AWSManagedServicesCloudFormationAdminRole` 및 `AWSManagedServicesUpdateRole`가 지정된 계정에 프로비저닝됩니다.

3. 내부 페더레이션 프로세스를 사용하여 DCM 액세스가 필요한 사용자에게 적절한 역할을 할당합니다.

Note

원하는 수의 `SAMLIdentityProviders`, `AWS Services` 및 `IAM 엔터티(역할, 사용자 등)`를 지정하여 역할을 수임할 수 있습니다. `SAMLIdentityProviderARNs`, `IAMEntityARNs` 또는 중 하나 이상을 제공해야 합니다 `AWSServicePrincipals`. 자세한 내용은 회사의 IAM 부서 또는 AMS 클라우드 아키텍트(CA)에 문의하세요.

직접 변경 모드 IAM 역할 및 정책

계정에서 직접 변경 모드가 활성화되면 다음과 같은 새 IAM 엔터티가 배포됩니다.

`AWSManagedServicesCloudFormationAdminRole`: 이 역할은 `CloudFormation` 콘솔에 대한 액세스 권한을 부여하고, `CloudFormation` 스택을 생성 및 업데이트하고, 드리프트 보고서를 보고, `CloudFormation ChangeSets`를 생성 및 실행합니다. 이 역할에 대한 액세스는 SAML 공급자를 통해 관리됩니다.

역할에 `AWSManagedServicesCloudFormationAdminRole` 배포되고 연결된 관리형 정책은 다음과 같습니다.

- AMS 고급 다중 계정 랜딩 존(MALZ) 애플리케이션 계정
 - `AWSManagedServices_CloudFormationAdminPolicy1`
 - `AWSManagedServices_CloudFormationAdminPolicy2`
 - 이 정책은에 부여된 권한을 나타냅니다 `AWSManagedServicesCloudFormationAdminRole`. 사용자와 파트너는 이 정책을 사용하여 계정의 기존 역할에 대한 액세스 권한을 부여하고 해당 역할이 계정의 `CloudFormation` 스택을 시작하고 업데이트하도록 허용합니다. 다른 IAM 엔터티가 `CloudFormation` 스택을 시작하도록 허용하려면 추가 AMS 서비스 제어 정책(SCP) 업데이트가 필요할 수 있습니다.
- AMS 고급 단일 계정 랜딩 존(SALZ) 계정

- AWSManagedServices_CloudFormationAdminPolicy1
- AWSManagedServices_CloudFormationAdminPolicy2
- cdk-legacy-mode-s3-access[인라인 정책]
- AWS ReadOnlyAccess 정책

AWSManagedServicesUpdateRole: 이 역할은 다운스트림 AWS 서비스 APIs에 대한 제한된 액세스 권한을 부여합니다. 역할은 변경 및 비변환 API 작업을 제공하는 관리형 정책과 함께 배포되지만, 일반적으로 IAM, KMS, GuardDuty, VPC, AMS 인프라 리소스 및 구성 등과 같은 특정 서비스에 대해 변경 작업(예: Create/Delete/PUT)을 제한합니다. 이 역할에 대한 액세스는 SAML 공급자를 통해 관리됩니다.

역할에 AWSManagedServicesUpdateRole 배포되고 연결된 관리형 정책은 다음과 같습니다.

- AMS Advanced 다중 계정 랜딩 존 애플리케이션 계정
 - AWSManagedServicesUpdateBasePolicy
 - AWSManagedServicesUpdateDenyPolicy
 - AWSManagedServicesUpdateDenyProvisioningPolicy
 - AWSManagedServicesUpdateEC2AndRDSPolicy
 - AWSManagedServicesUpdateDenyActionsOnAMSIInfraPolicy
- AMS Advanced 단일 계정 랜딩 존 계정
 - AWSManagedServicesUpdateBasePolicy
 - AWSManagedServicesUpdateDenyProvisioningPolicy
 - AWSManagedServicesUpdateEC2AndRDSPolicy
 - AWSManagedServicesUpdateDenyActionsOnAMSIInfraPolicy1
 - AWSManagedServicesUpdateDenyActionsOnAMSIInfraPolicy2

이 외에도 관리형 정책 AWSManagedServicesUpdateRole 역할에는 AWS 관리형 정책이 ViewOnlyAccess 연결되어 있습니다.

보안 및 규정 준수

보안 및 규정 준수는 AMS Advanced와 고객 간의 공동 책임입니다. AMS 고급 직접 변경 모드는 이 공동 책임을 변경하지 않습니다.

직접 변경 모드의 보안

AMS Advanced는 규범적 랜딩 존, 변경 관리 시스템 및 액세스 관리를 통해 추가 가치를 제공합니다. 직접 변경 모드를 사용하는 경우이 책임 모델은 변경되지 않습니다. 그러나 추가 위험을 알고 있어야 합니다.

직접 변경 모드 "업데이트" 역할(참조 [직접 변경 모드 IAM 역할 및 정책](#))은 계정 내에서 AMS 지원 서비스의 인프라 리소스를 변경할 수 있도록 엔터티가 액세스할 수 있는 승격된 권한을 제공합니다. 권한이 높아지면 리소스, 서비스 및 작업에 따라 다양한 위험이 존재합니다. 특히 감독, 실수 또는 내부 프로세스 및 제어 프레임워크 준수 부족으로 인해 잘못된 변경이 이루어지는 상황에서는 더욱 그렇습니다.

AMS 기술 표준에 따라 다음과 같은 위험이 식별되었으며 권장 사항은 다음과 같습니다. AMS 기술 표준에 대한 자세한 내용은 통해 확인할 수 있습니다 AWS Artifact. 에 액세스하려면 CSDM에 AWS Artifact문의하여 지침을 받거나 [시작하기로 AWS Artifact](#) 이동합니다.

AMS-STD-001: 태그 지정

표준	깨졌나요?	위험	권장 사항
모든 AMS 소유 리소스에는 다음과 같은 키-값 페어가 있어야 합니다.	예. CloudFormation, CloudTrail, EFS, OpenSearch, CloudWatch Logs, SQS, SSM, Tagging api에 대한 중단 - 이러한 서비스는 AMS 네임스페이스에 대한 태깅을 제한하는 aws:TagsKey 조건을 지원하지 않습니다.	AMS 리소스의 잘못된 태그 지정은 AMS 측 리소스의 보고, 알림 및 패치 적용 작업에 부정적인 영향을 미칠 수 있습니다.	AMS 팀 이외의 모든 사용자의 AMS 기본 태그 지정 요구 사항을 변경하려면 액세스를 재시도해야 합니다.
위에 나열된 태그 이외의 모든 AMS 소유 태그에는 upper/lower/mix스 대/소문자AMS*MC*와 같은 접두사가 있어야 합니다.	다음 표 AMS-STD-003에 제공된 표준은 AppId, 환경 및 AppName을 변경할 수 있지만 AMS 소유 리소스의 경우 변경할 수 없다고 명시합니다.		

표준	깨졌나요?	위험	권장 사항
AMS 소유 스택의 태그는 변경 요청에 따라 삭제해서는 안 됩니다.	IAM 권한을 통해 달성할 수 없습니다. 예. CloudFormation은 AMS 네임스페이스에 대한 태그를 제한하는 <code>aws:TagsKey</code> 조건을 지원하지 않습니다.		
다음 표 AMSAMS-STD-002 태그 이름 지정 규칙을 사용할 수 없습니다.	예. CloudFormation, CloudTrail, Amazon Elastic File System(EFS), OpenSearch, CloudWatch Logs, Amazon Simple Queue Service(SQS), Amazon EC2 Systems Manager(SM), 태그 지정 API에 대한 중단. 이러한 서비스는 AMS 네임스페이스에 대한 태그 지정을 제한하는 <code>aws:TagsKey</code> 조건을 지원하지 않습니다.		

AMS-STD-002: Identity and Access Management(IAM)

표준	깨졌나요?	위험	권장 사항
4.7 변경 관리 프로세스(RFC)를 우회하는 작업은 인스턴스 시작 또는 중지, S3 버킷 또	예. 셀프 서비스 작업의 목적을 통해 AMS RFC 시스템을 우회하	보안 액세스 모델은 AMS의 핵심 기술 패킷이며 콘솔 또는 프로그래밍 방식의 액세스	IAM 사용자는 시간 제한을 두고 최소 권한과 need-to-know 따라 권

표준	깨졌나요?	위험	권장 사항
는 RDS 인스턴스 생성 등과 같이 허용되지 않아야 합니다. 개발자 모드 계정 및 셀프 서비스 프로비저닝 모드 서비스(SSPS)는 작업이 할당된 역할의 경계 내에서 수행되는 한 면제됩니다.	는 작업을 수행할 수 있습니다.	스를 위한 IAM 사용자는 이 액세스 제어를 우회합니다. IAM 사용자 액세스는 AMS 변경 관리에서 모니터링되지 않습니다. 액세스는 CloudTrail에만 로깅됩니다.	한을 부여받아야 합니다.

AMS-STD-003: 네트워크 보안

표준	깨졌나요?	위험	권장 사항
S2. EC2 인스턴스의 탄력적 IP는 공식 위험 수락 계약 또는 내부 팀의 유효한 사용 사례에서만 사용해야 합니다.	예. 셀프 서비스 작업을 사용하면 탄력적 IP 주소(EIP)를 연결하고 연결을 해제할 수 있습니다.	인스턴스에 탄력적 IP를 추가하면 인스턴스가 인터넷에 노출됩니다. 이렇게 하면 정보 공개 및 무단 활동의 위험이 증가합니다.	보안 그룹을 통해 해당 인스턴스에 대한 불필요한 트래픽을 차단하고 보안 그룹이 인스턴스에 연결되어 있는지 확인하여 비즈니스상의 이유로 필요한 경우에만 트래픽을 허용하도록 합니다.
S14. 동일한 고객에게 속한 계정 간의 VPC 피어링 및 엔드포인트 연결을 허용할 수 있습니다.	예. IAM 정책을 통해 불가능합니다.	AMS 계정에서 나가는 트래픽은 계정 경계를 벗어나면 모니터링되지 않습니다.	소유하고 있는 AMS 계정으로만 피어링하는 것이 좋습니다. 사용 사례에 필요한 경우 보안 그룹 및 라우팅 테이블을 사용하여 관련 연결을 통해 송신할 수 있는 트래픽 범위, 리소스 및 유형을 제한합니다.

표준	깨졌나요?	위험	권장 사항
AMS 기본 AMIs는 동일한 AWS 조직에서 소유하고 있는지 확인할 수 있는 한 AMS 관리형 계정과 비관리형 계정 간에 공유할 수 있습니다.		AMIs 민감한 데이터가 포함될 수 있으며 의도하지 않은 계정에 노출될 수 있습니다.	조직 외부에서 공유하기 전에 조직이 소유한 계정과만 AMIs를 공유하거나 사용 사례 및 계정 정보를 검증합니다.

AMS-STD-007: 로깅

표준	깨졌나요?	위험	권장 사항
19. 모든 로그는 한 AMS 계정에서 동일한 고객의 다른 AMS 계정으로 전달할 수 있습니다.			
20. 모든 로그는 내부 도구를 사용하여 동일한 AMS 고객이 비 AMS 계정을 소유한 경우에만(동일한 계정인지 AWS Organizations 확인하거나 이메일 도메인을 고객의 회사 이름 및 PAYER 연결 계정과 일치시켜) AMS에서 비 AMS 계정으로 전달할 수 있습니다.	예. 동일한 조직에 있는 고객 계정의 확인으로 인한 고객 로그의 잠재적 비보안은 IAM 정책을 통해 달성할 수 없습니다.	로그에는 민감한 데이터가 포함될 수 있으며 의도하지 않은 계정에 노출될 수 있습니다.	조직 외부에서 공유하기 전에 AWS 조직에서 관리하는 계정과만 로그를 공유하거나 사용 사례 및 계정 정보를 검증합니다. 이를 여러 가지 방법으로 확인할 수 있습니다. 클라우드 서비스 제공 관리자(CSDM)에게 문의하십시오.

이에 따라 내부 권한 부여 및 인증 팀과 협력하여 Direct Change 모드 역할에 대한 권한을 제어합니다.

직접 변경 모드의 규정 준수

Direct Change 모드는 프로덕션 워크로드와 비프로덕션 워크로드 모두와 호환됩니다. 규정 준수 표준 (예: PHI, HIPAA, PCI)을 준수하고 Direct Change 모드 사용이 내부 제어 프레임워크 및 표준을 준수하도록 하는 것은 사용자의 책임입니다.

직접 변경 모드에서 변경 관리

변경 관리는 AMS Advanced가 변경 요청을 구현하는 데 사용하는 프로세스입니다. 변경 요청(RFC)은 관리형 환경을 변경하기 위해 사용자 또는 AMS Advanced 인터페이스를 통해 AMS Advanced가 생성한 요청이며 특정 작업에 대한 AMS Advanced 변경 유형(CT) ID를 포함합니다. 자세한 내용은 [변경 관리를 참조](#)하세요.

Note

직접 변경 모드는 AMS 변경 관리 RFCs 제거하지 않으며 DCM을 사용하는 AMS RFCs에 대한 전체 액세스 권한을 여전히 가집니다.

AMS Direct Change 모드(DCM)는 AWS 리소스를 프로비저닝하고 업데이트하기 위해 AMS Advanced Plus 및 Premium 계정에 대한 기본 AWS 액세스를 제공하여 AMS Advanced 변경 관리를 확장합니다. IAM 역할을 통해 Direct Change 모드 권한을 부여받은 사용자는 기본 AWS API 액세스를 사용하여 AMS Advanced 계정의 리소스를 프로비저닝하고 변경할 수 있습니다. 사용자는 동일한 IAM 역할을 사용하여 AMS Advanced 변경 관리 RFCs를 계속 사용할 수 있습니다. 두 경우 모두 모니터링, 패치, 백업, 인시던트 대응 관리를 포함하여 AMS에서 리소스와 리소스 변경 사항을 완벽하게 지원합니다. 이러한 계정에서 적절한 역할이 없는 사용자는 AMS Advanced 변경 관리 RFC 프로세스를 사용하여 변경해야 합니다.

변경 관리 사용 사례

보안상의 이유로 AMS Advanced의 일부 변경은 변경 관리 변경 요청(RFC) 프로세스를 통해서만 수행할 수 있습니다. `AWSManagedServicesCloudFormationAdminRole`는 `CloudFormation(CFN)`을 통해 수행되는 작업으로 제한됩니다. DCM을 통해 스택을 생성하는 방법에 대한 자세한 내용은 [Direct Change 모드를 사용하여 스택 생성을 참조](#)하세요. `AWSManagedServicesUpdateRole`는 다음 작업으로 제한됩니다.

관리 | 관리형 계정 | 직접 변경 모드 | 활성화(ct-3rd4781c2nnhp) 변경 유형을 포함한 각 변경 유형에 대한 예제 안내는 분류별 AMS 고급 변경 유형 참조 변경 유형 섹션에서 관련 변경 유형에 대

한 "추가 정보" 섹션을 참조하세요. <https://docs.aws.amazon.com/managedservices/latest/ctref/classifications.html>

서비스:	작업
AWS Key Management Service (AWS KMS)	업데이트
AWS Certificate Manager	생성
AWS Identity and Access Management (IAM)	모두
AWS VPN	임의
AMS 리소스 스케줄러	
AWS Backup	백업 계획 생성
AMS 워크로드 수집(WIGs)	임의
AMS 송신 필터링(Managed Palo Alto)	
AMS Advanced MALZ 계정 변경 사항	
Amazon GuardDuty	임의
AMS 고급 스택 액세스	
Amazon Elastic Block Store(EBS) 볼륨	삭제
Amazon Elastic Block Store(EBS) 기본 암호화	기본 암호화 활성화
Amazon Elastic Compute Cloud(Amazon EC2)	호스트 이름 변경
Amazon Machine Image(AMI)	삭제, 공유
Amazon EC2 보안 그룹	임의
AMS 고급 SSPS	
AWS 관리형 Microsoft AD	
AMS Advanced 개발자 모드	

서비스:	작업
Amazon Simple Storage Service(S3)	S3 버킷 정책 생성
AWS Systems Manager	생성

Direct Change 모드를 사용하여 스택 생성

AMS에서 스택을 관리하려면 사용하여 CloudFormation에서 스택을 시작할 때 다음 두 가지 요구 사항이 있습니다 `AWSManagedServicesCloudFormationAdminRole`.

- 템플릿에는 `가` 포함되어야 합니다 `AmsStackTransform`.
- 스택 이름은 접두사 뒤에 17자의 영숫자 문자열 `stack-`로 시작해야 합니다.

Note

를 성공적으로 사용하려면 스택 템플릿에 AWS CloudFormation (CFN)가 스택을 생성하거나 업데이트하기 위한 `CAPABILITY_AUTO_EXPAND` 기능이 포함되어 있음을 확인해야 `AmsStackTransform`합니다. 이렇게 하려면 `create-stack` 요청의 `CAPABILITY_AUTO_EXPAND` 일부로 전달합니다. `가` 템플릿에 포함될 때 이 기능이 확인되지 않으면 `CFNAmsStackTransform`은 요청을 거부합니다. CFN 콘솔은 템플릿에 변환이 있는 경우가 기능을 전달하도록 보장하지만 APIs를 통해 CFN과 상호 작용할 때 이 기능을 놓칠 수 있습니다.

다음 CFN API 호출을 사용할 때마다 이 기능을 전달해야 합니다.

- [CreateChangeSet](#)
- [CreateStack](#)
- [UpdateStack](#)

DCM을 사용하여 스택을 생성하거나 업데이트할 때 스택에 대해 동일한 CFN 수집 및 스택 업데이트 CTs 검증 및 증강이 수행됩니다. 자세한 내용은 [AWS CloudFormation 수집 지침, 모범 사례 및 제한을 참조하세요](#). 단, AMS 기본 보안 그룹(SGs)은 독립형 EC2 인스턴스 또는 Auto Scaling 그룹(ASGs)의 EC2 인스턴스에 연결되지 않습니다. 독립형 EC2 인스턴스 또는 ASGs를 사용하여 CloudFormation 템플릿을 생성할 때 기본 SGs.

Note

이제를 사용하여 IAM 역할을 생성하고 관리할 수 있습니다.
다AWSManagedServicesCloudFormationAdminRole.

AMS 기본 SGs에는 인스턴스를 성공적으로 시작하고 나중에 AMS 작업 및 사용자에게 의해 SSH 또는 RDP를 통해 액세스할 수 있는 수신 및 송신 규칙이 있습니다. AMS 기본 보안 그룹이 너무 허용적이라고 판단되면 사용자와 AMS 작업이 인시던트 발생 시 인스턴스에 액세스할 수 있도록 허용하는 한 보다 제한적인 규칙을 사용하여 자체 SGs를 생성하고 인스턴스에 연결할 수 있습니다.

AMS 기본 보안 그룹은 다음과 같습니다.

- SentinelDefaultSecurityGroupPrivateOnly: 이 SSM 파라미터를 통해 CFN 템플릿에서 액세스할 수 있습니다. /ams/\${VpcId}/SentinelDefaultSecurityGroupPrivateOnly
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll: 이 SSM 파라미터를 통해 CFN 템플릿에서 액세스할 수 있습니다. /ams/\${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll

AMS 변환

CloudFormation 템플릿에 Transform 문을 추가합니다. 그러면 시작 시 스택을 검증하고 AMS에 등록하는 CloudFormation 매크로가 추가됩니다.

JSON 예제

```
"Transform": {
  "Name": "AmsStackTransform",
  "Parameters": {
    "StackId": {"Ref" : "AWS::StackId"}
  }
}
```

YAML 예제

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

또한 기존 스택의 템플릿을 업데이트할 때 Transform 문을 추가합니다.

JSON 예제

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
  "Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

YAML 예제

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
```

```
Type: AWS::SNS::Topic
Properties:
  TopicName: !Ref TopicName
```

스택 이름

스택 이름은 접두사 뒤에 17자의 영숫자 문자열stack-로 시작해야 합니다. 이는 AMS 스택 IDs.

다음은 호환되는 스택 IDs.

Bash:

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python:

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell:

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17 | %
{[char]$_}) )
```

직접 변경 모드 사용 사례

다음은 직접 변경 모드의 사용 사례입니다.

를 통한 리소스 프로비저닝 및 관리 AWS CloudFormation

- 기존 CloudFormation 기반 도구 및 프로세스를 통합합니다.

지속적인 리소스 관리 및 업데이트

- 위험이 낮은 작은 원자성 변화.
- 수동 또는 자동 RFC를 통해 실행되는 변경 사항입니다.

- 네이티브 AWS API 액세스가 필요한 도구입니다.
- 마이그레이션 단계에 있는 경우 DCM 역할을 사용할 수 있습니다. 마이그레이션 팀은 DCM에 대한 권한을 활용하여 스택을 생성하거나 수정합니다.
- CI/CD 파이프라인에서 DCM 역할을 사용하여 새 AMIs를 빌드하고 Amazon ECS 작업을 생성하는 등의 작업을 수행할 수 있습니다.

AMS 고급 개발자 모드

주제

- [AMS Advanced Developer 모드 시작하기](#)
- [개발자 모드의 보안 및 규정 준수](#)
- [개발자 모드의 변경 관리](#)
- [AMS 개발자 모드에서 인프라 프로비저닝](#)
- [AMS 개발자 모드의 탐지 제어](#)
- [AMS 개발자 모드에서 로깅, 모니터링 및 이벤트 관리](#)
- [AMS 개발자 모드에서의 인시던트 관리](#)
- [AMS 개발자 모드에서 패치 관리](#)
- [AMS 개발자 모드에서 연속성 관리](#)
- [AMS 개발자 모드의 보안 및 액세스 관리](#)

AWS Managed Services(AMS) 개발자 모드는 AMS Advanced Plus 및 Premium 계정에서 승격된 권한을 사용하여 AMS Advanced 변경 관리 프로세스 외부에서 AWS 리소스를 프로비저닝하고 업데이트합니다. AMS Advanced Developer 모드는 AMS Advanced Virtual Private Cloud(VPC) 내의 네이티브 AWS API 호출을 활용하여 이를 수행하므로 관리형 환경에서 인프라와 애플리케이션을 설계하고 구현할 수 있습니다.

개발자 모드가 활성화된 계정을 사용하는 경우 AMS Advanced 변경 관리 프로세스를 통해 또는 AMS Amazon Machine Image(AMI)를 사용하여 프로비저닝된 리소스에 대해 연속성 관리, 패치 관리 및 변경 관리가 제공됩니다. 그러나 이러한 AMS 관리 기능은 AWS APIs 통해 프로비저닝된 리소스에는 제공되지 않습니다.

사용자는 AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝되는 인프라 리소스를 모니터링할 책임이 있습니다. 개발자 모드는 프로덕션 워크로드와 비프로덕션 워크로드 모두와 호환됩니다. 권한이 승격되면 내부 제어를 준수할 책임이 증가합니다.

⚠ Important

개발자 모드를 사용하여 생성한 리소스는 AMS Advanced 변경 관리 프로세스를 사용하여 생성한 경우에만 AMS Advanced에서 관리할 수 있습니다.

개발자 모드는 사용할 수 있는 AMS 고급 모드 중 하나입니다. 자세한 내용은 [모드 개요](#) 단원을 참조하십시오.

AMS Advanced Developer 모드 시작하기

AMS Advanced Developer 모드가 있는 다양한 AMS Advanced 계정과 개발자 모드를 성공적으로 구현하는 방법을 알아봅니다.

주제

- [AMS 개발자 모드를 시작하기 전에](#)
- [AMS 개발자 모드의 사전 조건](#)
- [AMS Advanced Developer 모드를 구현하는 방법](#)
- [AMS 고급 개발자 모드 권한](#)

AMS 개발자 모드를 시작하기 전에

개발자 모드를 구현하기 전에 알아야 할 몇 가지 사항이 있습니다.

AMS Advanced는 변경 요청(RFCs)을 통해 AMS Advanced 변경 관리 프로세스 외부에서 생성된 DevMode 계정의 기존 스택 또는 리소스를 관리할 수 없습니다. 그러나 계정이 DevMode에 있는 동안 AMS Advanced는 RFCs를 사용하여 AMS Advanced 변경 관리 프로세스를 통해 프로비저닝된 리소스를 계속 관리합니다.

DevMode 계정으로 시작하여 나중에 AMS Advanced 관리형 애플리케이션 계정으로 은폐할 수 없습니다.

AMS 개발자 모드의 사전 조건

다음은 개발자 모드를 구현하기 위한 사전 조건입니다.

- 온보딩된 AMS Advanced Plus 또는 Premium 계정이 하나 이상 있는 AMS Advanced 고객이어야 합니다.

- 사용하는 모든 계정은 AMS Advanced Plus 또는 Premium 계정이어야 합니다.
- 다중 계정 랜딩 존(MALZ): AWSManagedServicesDevelopmentRole 사전 정의된 AWS Identity and Access Management (IAM) 역할을 사용해야 합니다. 이 역할을 요청합니다. 다음 섹션에서는 개발자 모드 권한을 획득하는 방법을 설명합니다.
- 단일 계정 랜딩 존(SALZ): customer_developer_role 사전 정의된 AWS Identity and Access Management (IAM) 역할을 사용해야 합니다. 이 역할을 요청합니다. 다음 섹션에서는 개발자 모드 권한을 획득하는 방법을 설명합니다.

AMS Advanced Developer 모드를 구현하는 방법

적합한 AMS Advanced 계정에 사전 정의된 IAM 역할을 프로비저닝하도록 요청하여 개발자 모드를 구현합니다.

- MALZ: AWSManagedServicesDevelopmentRole
- SALZ: customer_developer_role

그런 다음 페더레이션 네트워크의 관련 사용자에게 역할을 할당합니다.

개발자 모드는 AMS 고급 관리형 리소스에 대한 AMS 고급 변경 관리와 고객이 관리하는 리소스에 대한 고객 관리형 역할 페더레이션이라는 두 가지 변경 벡터를 생성하므로 개발자 모드 사용이 내부 제어 프레임워크 및 표준을 준수하는지 확인하는 것이 좋습니다. AMS Advanced 프로세스는 선언을 계속 준수하지만 고객 프로세스 및 제어 프레임워크를 업데이트해야 할 수 있습니다.

AMS Advanced 계정에서 개발자 모드를 구현하려면

1. 개발자 모드와 함께 사용할 계정에 나열된 요구 사항을 충족하는지 확인합니다. [AMS 개발자 모드의 사전 조건](#).
2. 변경 유형(CT) 관리 | 관리형 계정 | 개발자 모드 | 활성화(검토 필요)를 사용하여 변경 요청(RFC)을 제출합니다. 이 CT를 사용하는 방법의 예는 [개발자 모드 | 활성화\(검토 필요\)](#)를 참조하세요.

CT가 처리되면 미리 정의된 IAM 역할(AWSManagedServicesDevelopmentRoleMALZ의 경우, SALZ의 customer_developer_role 경우)이 요청된 계정에 프로비저닝됩니다.

3. 내부 페더레이션 프로세스를 사용하여 개발자 모드 액세스가 필요한 사용자에게 적절한 역할을 할당합니다.

AMS Advanced는 리소스의 원치 않거나 승인되지 않은 프로비저닝 또는 변경을 방지하기 위해 액세스를 제한할 것을 권장합니다.

AMS 고급 개발자 모드 권한

사전 정의된 역할(AWSManagedServicesDevelopmentRoleMALZ의 경우, SALZ의 customer_developer_role 경우)은 AMS Advanced에서 운영하는 공유 서비스 구성 요소(예: 관리 호스트, 도메인 컨트롤러, Trend Micro EPS, 접속 및 지원되지 않는 AWS 서비스)에 대한 액세스를 제한하면서 IAM 역할을 포함하여 AMS Advanced VPC 내에 애플리케이션 인프라 리소스를 생성할 수 있는 권한을 부여합니다. 또한 역할은 AWS 서비스 Amazon GuardDuty, AWS Organizations, AWS Directory Service APIs.

역할을 통해 추가 IAM 역할을 생성할 수 있지만 개발자 모드 액세스에 포함된 것과 동일한 권한 경계에서 생성한 모든 IAM 역할에 적용됩니다AWSManagedServicesDevelopmentRole.

개발자 모드의 보안 및 규정 준수

보안 및 규정 준수는 AMS Advanced와 고객 간의 공동 책임입니다. AMS 고급 개발자 모드는 변경 관리 프로세스 외부에서 프로비저닝되거나 변경 관리를 통해 프로비저닝되지만 개발자 모드 권한으로 업데이트된 리소스에 대한 공동 책임을 사용자에게 이전합니다. 공동 책임에 대한 자세한 내용은 [AWS Managed Services](#)를 참조하세요.

주의:

- DevMode를 사용하면 사용자와 권한 있는 팀이 AMS 보안의 핵심에서 deny-by-default 원칙을 우회할 수 있습니다. AMS 대기 시간이 짧고 셀프 서비스라는 이점은 단점과 비교해야 합니다. 누구나 보안 팀에 알리지 않고도 예기치 않고 파괴적인 작업을 수행할 수 있습니다. 개발 모드 및 직접 변경 모드를 활성화하는 자동 변경 유형이 노출되며, 조직 내 권한이 있는 모든 사람이 이러한 CTs 실행하고 이러한 모드를 활성화할 수 있습니다.
- 사용자 기반에서 CT 실행 권한을 관리할 책임은 사용자에게 있습니다.
- AMS는 CT 실행 권한을 관리하지 않습니다.

권장 사항:

- 보호
 - 고객은 권한을 통해이 CT에 대한 액세스를 차단할 수 있습니다. [IAM 역할 정책 설명을 사용하여 권한 제한](#)을 참조하세요.
 - ITSM 시스템과 같은 프록시를 구현하여이 CT에 대한 액세스 방지
 - 필요에 따라 정책 및 동작을 방지하는 서비스 제어 정책(SCPs)을 활용합니다. [AMS 예방 및 탐지 제어 라이브러리](#)를 참조하세요.

- 감지
 - RFC에서 실행 중인 CTs(개발자 모드 ct-1opjmhuddw194 및 직접 변경 모드 활성화, ct-3rd4781c2nnhp 활성화)를 모니터링하고 그에 따라 응답합니다.
 - 계정에서 IAM 리소스가 있는지 검토 및/또는 감사하여 개발자 모드 또는 직접 변경 모드가 배포된 계정을 식별합니다.
- 응답
 - 필요에 따라 개발자 모드에서 계정 제거

개발자 모드의 보안

AMS Advanced는 규범적 랜딩 존, 변경 관리 시스템 및 액세스 관리를 통해 추가 가치를 제공합니다. 개발자 모드를 사용하는 경우 AMS Advanced의 보안 값은 기본 AMS Advanced 보안 강화 네트워크를 설정하는 표준 AMS Advanced 계정과 동일한 계정 구성을 사용하여 유지됩니다. 네트워크는 역할(AWSManagedServicesDevelopmentRoleMALZ의 경우, SALZ의 customer_developer_role 경우)에 적용되는 권한 경계로 보호되므로 사용자가 계정을 설정할 때 설정된 파라미터 보호 기능을 분해하지 못하도록 제한됩니다.

예를 들어 역할이 있는 사용자는 Amazon Route 53에 액세스할 수 있지만 AMS Advanced 내부 호스팅 영역은 제한됩니다. 에서 생성한 IAM 역할에도 동일한 권한 경계가 적용되어 계정이 AMS Advanced에 온보딩될 때 설정된 파라미터 보호 기능을 사용자가 분해하지 못하도록 제한AWSManagedServicesDevelopmentRole하는에 권한 경계를 AWSManagedServicesDevelopmentRole적용합니다.

개발자 모드의 규정 준수

개발자 모드는 프로덕션 워크로드와 비프로덕션 워크로드 모두와 호환됩니다. 규정 준수 표준(예: PHI, HIPAA, PCI)을 준수하고 개발자 모드 사용이 내부 제어 프레임워크 및 표준을 준수하도록 하는 것은 사용자의 책임입니다.

개발자 모드의 변경 관리

변경 관리는 AMS Advanced 서비스가 변경 요청을 구현하는 데 사용하는 프로세스입니다. 변경 요청(RFC)은 관리형 환경을 변경하기 위해 AMS Advanced 인터페이스를 통해 사용자 또는 AMS Advanced가 생성하는 요청이며 특정 작업에 대한 변경 유형(CT) ID를 포함합니다. 자세한 내용은 [변경 관리 모드](#) 단원을 참조하십시오.

개발자 모드 권한이 부여된 AMS Advanced 계정에서는 변경 관리가 적용되지 않습니다. IAM 역할(AWSManagedServicesDevelopmentRoleMALZ의 경우, SALZ의 customer_developer_role

경우)로 개발자 모드 권한을 부여받은 사용자는 기본 AWS API 액세스를 사용하여 AMS Advanced 계정의 리소스를 프로비저닝하고 변경할 수 있습니다. 이러한 계정에서 적절한 역할이 없는 사용자는 AMS Advanced 변경 관리 프로세스를 사용하여 변경해야 합니다.

Important

개발자 모드를 사용하여 생성한 리소스는 AMS Advanced 변경 관리 프로세스를 사용하여 생성한 경우에만 AMS Advanced에서 관리할 수 있습니다. AMS Advanced 변경 관리 프로세스 외부에서 생성된 리소스에 대해 AMS Advanced에 제출된 변경 요청은 사용자가 처리해야 하므로 AMS Advanced에서 거부합니다.

셀프 서비스 프로비저닝 서비스 API 제한

모든 AMS Advanced 자체 프로비저닝 서비스는 개발자 모드에서 지원됩니다. 자체 프로비저닝된 서비스에 대한 액세스에는 각 사용 설명서 섹션에 설명된 제한 사항이 적용됩니다. 개발자 모드 역할에서 자체 프로비저닝된 서비스를 사용할 수 없는 경우 개발자 모드 변경 유형을 통해 업데이트된 역할을 요청할 수 있습니다.

다음 서비스는 서비스 APIs에 대한 전체 액세스를 제공하지 않습니다.

개발자 모드에서 제한된 자체 프로비저닝 서비스

서비스:	참고
Amazon API Gateway	APIs 호출이 허용됩니다SetWebACL .
Application Auto Scaling	확장 가능 대상만 등록 또는 등록 취소하고 조정 정책을 추가 또는 삭제할 수 있습니다.
AWS CloudFormation	접두사가 인 이름이 있는 CloudFormation 스택에는 액세스하거나 수정할 수 없습니다mc-.
AWS CloudTrail	ams- 및/또는 접두사가 붙은 이름이 있는 CloudTrail 리소스에는 액세스하거나 수정할 수 없습니다mc-.
Amazon Cognito(사용자 풀)	소프트웨어 토큰을 연결할 수 없습니다.

서비스:	참고
	사용자 풀, 사용자 가져오기 작업, 리소스 서버 또는 자격 증명 공급자를 생성할 수 없습니다.
AWS Directory Service	Connect 및 WorkSpaces 서비스에는 다음 AWS Directory Service 작업만 필요합니다. 다른 모든 디렉터리 서비스 작업은 개발자 모드 권한 경계 정책에 의해 거부됩니다. • ds:AuthorizeApplication • ds:CreateAlias • ds:CreateIdentityPoolDirectory • ds>DeleteDirectory • ds:DescribeDirectories • ds:GetAuthorizedApplicationDetails • ds:ListAuthorizedApplications • ds:UnauthorizeApplication 단일 계정 랜딩 존 계정에서 경계 정책은 개발 모드 활성화 계정에 대한 액세스를 유지하기 위해 AMS Advanced에서 사용하는 AMS Advanced 관리형 디렉터리에 대한 액세스를 명시적으로 거부합니다.
Amazon Elastic Compute Cloud	, DhcpOptions , Gateway, 및 문자열이 포함된 Amazon EC2 APIsSubnet에 액세스할 수 없습니다VPCVPN. AMS, ManagementHostASG , 및/또는 접두사가 붙은 태그가 있는 Amazon EC2 리소스mc에는 액세스하거나 수정할 수 없습니다sentinel.

서비스:	참고
Amazon EC2(보고서)	보기 액세스 권한만 부여됩니다(수정할 수 없음). 참고: Amazon EC2 보고서가 이동 중입니다. 보고서 메뉴 항목은 Amazon EC2 콘솔 탐색 메뉴에서 제거됩니다. Amazon EC2 사용 보고서를 제거한 후 보려면 AWS Billing 및 비용 관리 콘솔을 사용합니다.
AWS Identity and Access Management (IAM)	기존 권한 경계를 삭제하거나 IAM 사용자 암호 정책을 수정할 수 없습니다. 올바른 IAM 역할(AWSManagedServicesDevelopmentRole MALZ의 경우, customer_developer_role SALZ의 경우)을 사용하지 않는 한 IAM 리소스를 생성하거나 수정할 수 없습니다. ams, mccustomer_deny_policy, 및/또는 접두사가 붙은 IAM 리소스는 수정할 수 없습니다 sentinel. 새 IAM 리소스(역할, 사용자 또는 그룹)를 생성할 때 권한 경계(MALZ: AWSManagedServicesDevelopmentRolePermissionsBoundary, SALZ: ams-app-infra-permissions-boundary)를 연결해야 합니다.
AWS Key Management Service (AWS KMS)	AMS 고급 관리형 KMS 키에 액세스하거나 수정할 수 없습니다.
AWS Lambda	접두사가 인 AWS Lambda 함수에는 액세스하거나 수정할 수 없습니다AMS.
CloudWatch Logs(CloudWatch 로그)	이름 앞에 mc, lambda, 및/또는 접두사가 붙은 CloudWatch 로그 스트림aws에 액세스할 수 없습니다AMS.

서비스:	참고
Amazon Relational Database Service(Amazon RDS)	이름이 접두사인 Amazon Relational Database Service(RDS) 데이터베이스(DBs)에는 액세스 하거나 수정할 수 없습니다mc-.
AWS Resource Groups	Get, List 및 Search 리소스 그룹 API 작업에 만 액세스할 수 있습니다.
Amazon Route 53	Route53 AMS 고급 유지 관리 리소스에 액세스 하거나 수정할 수 없습니다.
Amazon S3	ams-*, , ams ms-a 또는 접두사가 붙은 이름이 있는 Amazon S3 버킷에는 액세스할 수 없습니다mc-a.
AWS Security Token Service	허용되는 유일한 보안 토큰 서비스 API는 DecodeAuthorizationMessage .
Amazon SNS	이름이 접두사 AMS-, Energion-Topic 또는 인 SNS 주제에 액세스할 수 없습니다MMS-Topic .
AWS Systems Manager 관리자(SSM)	ams, mc 또는 접두사가 붙은 SSM 파라미터는 수정할 수 없습니다svc. ams 또는 접두사가 붙은 태그가 있는 Amazon EC2 인스턴스SendCommand 에는 SSM API를 사용할 수 없습니다mc.
AWS 태그 지정	접두사가 인 AWS API 작업 태그 지정에만 액세스할 수 있습니다Get.

서비스:	참고
AWS Lake Formation	다음 AWS Lake Formation API 작업은 거부됩니다. • <code>lakeformation:DescribeResource</code> • <code>lakeformation:GetDataLakeSettings</code> • <code>lakeformation:DeregisterResource</code> • <code>lakeformation:RegisterResource</code> • <code>lakeformation:UpdateResource</code> • <code>lakeformation:PutDataLakeSettings</code>
Amazon Elastic Inference	Elastic Inference API 작업 만 호출할 수 있습니다. <code>elastic-inference:Connect</code> . 이 권한은 <code>customer_sagemaker_admin_policy</code> 연결된에 포함됩니다. <code>customer_sagemaker_admin_role</code> . 이 작업을 통해 Elastic Inference 액셀러레이터에 액세스할 수 있습니다.
AWS Shield	이 서비스 APIs 또는 콘솔에는 액세스할 수 없습니다.
Amazon Simple Workflow Service	이 서비스 APIs 또는 콘솔에는 액세스할 수 없습니다.

AMS 개발자 모드에서 인프라 프로비저닝

개발자 모드 IAM 역할이 없는 사용자는 개발자 모드가 활성화된 계

정 `AWSManagedServicesDevelopmentRole`에서 AMS Advanced AMIs. 올바른 역할(MALZ: `AWSManagedServicesDevelopmentRole`, SALZ: `customer_developer_role`)을 가진 사용자는 AMS Advanced 변경 관리 시스템 및 AMS Advanced AMIs 사용할 수 있지만 필수는 아닙니다.

Note

AWS AMS Advanced 워크로드 수집을 통해 처리되지 않았거나 AMS Advanced 계정에서 생성되지 않은 AMI에는 AMS Advanced 필수 구성이 포함되지 않습니다.

AMS 개발자 모드의 탐지 제어

이 섹션에는 민감한 AMS 보안 관련 정보가 포함되어 있으므로 수정되었습니다. 이 정보는 AMS 콘솔 설명서를 통해 확인할 수 있습니다. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 [AWS 아티팩트 시작하기](#)를 참조하세요.

AMS 개발자 모드에서 로깅, 모니터링 및 이벤트 관리

로깅, 모니터링 및 이벤트 관리는 AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에는 사용할 수 없습니다.

AMS 개발자 모드에서의 인시던트 관리

인시던트 대응 시간은 변경되지 않습니다. 인시던트 해결은 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에 대한 최선의 작업입니다.

Note

AMS 서비스 수준 계약(SLA)은 AMS 변경 관리 시스템 외부에서 생성되거나 업데이트된 리소스(변경 요청 또는 RFCs), 개발자 모드 포함에 적용되지 않으므로 개발자 모드에서 업데이트되거나 생성된 리소스는 P3로 자동 저하되며 AMS 지원이 최선의 노력입니다.

AMS 개발자 모드에서 패치 관리

AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에는 패치 관리를 사용할 수 없습니다. 패치 적용 시간:

- 중요한 보안 업데이트의 경우: 변경 관리를 통해 프로비저닝된 후 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에 대해 공급업체가 릴리스한 후 영업일 기준 10일 이내.
- 중요한 업데이트의 경우: 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에 대해 공급업체가 릴리스한 후 2개월 이내.

AMS 개발자 모드에서 연속성 관리

AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에는 연속성 관리를 사용할 수 없습니다.

환경 복구 시작 시간은 AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 후 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스의 경우 최대 12 시간이 걸릴 수 있습니다.

AMS 개발자 모드의 보안 및 액세스 관리

맬웨어 방지 보호는 AMS Advanced 변경 관리 프로세스 외부에서 프로비저닝된 리소스 또는 변경 관리를 통해 프로비저닝된 다음 개발자 모드 권한을 사용하여 계정에 의해 변경된 리소스에 대한 사용자의 책임입니다. AMS Advanced 변경 관리를 통해 프로비저닝되지 않은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 대한 액세스는 페더레이션 액세스를 제공하는 대신 키 페어에 의해 제어될 수 있습니다.

AMS의 셀프 서비스 프로비저닝 모드

AWS Managed Services(AMS) 셀프 서비스 프로비저닝(SSP) 모드는 AMS 관리형 계정의 기본 AWS 서비스 및 API 기능에 대한 전체 액세스를 제공합니다. 표준화된 범위 축소 AWS Identity and Access Management 역할을 통해 서비스에 액세스합니다. AMS는 서비스 요청 및 인시던트 관리를 제공합니다. 알림, 모니터링, 로깅, 패치, 백업 및 변경 관리는 사용자의 책임입니다. 대부분의 경우 자체 서비스 프로비저닝 서비스(SSPS)는 자체 관리형 또는 서버리스 서비스이므로 패치 적용과 같은 특정 운영 작업을 관리할 필요가 없습니다. AMS 가드레일에 정의된 환경 경계 내에서 이러한 서비스를 사용하면 이점을 얻을 수 있으며, 플랫폼의 기본 보안을 유지하려면 모든 IAM 변경 사항(서비스 연결 역할, 서비스 역할, 교차 계정 역할 또는 정책 업데이트 포함)을 AMS Operations의 승인을 받아야 합니다. 템플릿을 활용하여 AWS CloudFormation 이러한 서비스의 배포를 자동화할 수 있지만 모든 SSP 서비스에서 지원되지는 않습니다.

⚠ Important

AWS Managed Services(AMS) 계정에서 SSP 모드를 사용하여 명시된 제한 사항에 따라 AWS 서비스에 액세스하고 서비스를 사용할 수 있습니다.

AMS 계정에는 AMS 관리 없이 사용할 수 있는 AWS 서비스 몇 가지가 있습니다. 셀프 서비스 프로비저닝 모드 서비스 또는 간단히 말해 SSPS, AMS 계정에 추가하는 방법 및 각 서비스에 대한 FAQs는 섹션에 설명되어 있습니다.

셀프 서비스 프로비저닝 서비스는 있는 그대로 제공되며 사용자는 이를 관리할 책임이 있습니다. AMS는 해당 서비스와 연결된 리소스에 대한 알림, 모니터링, 로깅 또는 패치를 제공하지 않습니다. AMS는 AMS 계정에서 서비스를 안전하게 사용할 수 있는 IAM 역할을 제공합니다. AMS SLAs는 적용되지 않습니다.

셀프 서비스를 통해 프로비저닝하는 리소스의 경우 AMS는 인시던트 관리, 탐지 제어 및 가드레일, 보고, 지정된 리소스(Cloud Service Delivery Manager 및 Cloud Architect), 보안 및 액세스, 서비스 요청을 통한 기술 지원을 제공합니다. 또한 해당하는 경우 AMS 변경 관리 시스템 외부에서 프로비저닝되거나 구성된 리소스의 연속성 관리, 패치 관리, 인프라 모니터링 및 변경 관리에 대한 책임을 집니다.

AMS에서 SSP 모드 시작하기

셀프 서비스 프로비저닝은 사용할 수 있는 다중 계정 랜딩 존(MALZ)의 AMS 모드 중 하나입니다. 자세한 내용은 [모드 개요](#) 단원을 참조하십시오.

셀프 서비스 프로비저닝 기능을 제공하기 위해 AMS는 권한 경계가 있는 승격된 IAM 역할을 생성하여 직접 AWS 서비스 액세스에서 의도하지 않은 변경을 제한했습니다. 역할이 모든 변경을 막는 것은 아니며, 내부 제어 및 규정 준수 정책을 준수하고 사용 AWS 서비스 중인 모든가 필수 인증을 충족하는지 확인해야 합니다. 셀프 서비스 프로비저닝 모드입니다. AWS 규정 준수 요구 사항에 대한 자세한 내용은 [AWS 규정 준수를](#) 참조하세요.

다중 계정 랜딩 존 애플리케이션 계정에 셀프 서비스 프로비저닝 서비스를 추가하려면 서비스에 대한 지침에 따라 검토가 필요한 CT 또는 자동 CT인 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형(CT) 추가를 사용합니다.

i Note

AMS가 추가 셀프 서비스 프로비저닝 서비스를 제공하도록 요청하려면 서비스 요청을 제출합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon API Gateway 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon API Gateway 기능에 직접 액세스할 수 있습니다. [Amazon API Gateway](#)는 어떤 규모에서든 개발자가 API를 손쉽게 생성, 게시, 유지 관리, 모니터링 및 보호할 수 있도록 지원하는 완전관리형 서비스입니다. 를 사용하면 애플리케이션이 Amazon Elastic Compute Cloud([Amazon EC2](#))에서 실행되는 워크로드,에서 실행되는 코드, [AWS Lambda](#) 웹 애플리케이션 또는 실시간 통신 애플리케이션과 같은 백엔드 서비스에서 데이터, 비즈니스 로직 또는 기능에 액세스할 수 있는 문 역할을 하는 REST 및 WebSocket APIs를 생성할 AWS Management Console 수 있습니다.

API Gateway는 트래픽 관리, 권한 부여 및 액세스 제어, 모니터링 및 API 버전 관리를 포함하여 최대 수십만 개의 동시 API 호출을 수락하고 처리하는 데 관련된 모든 작업을 처리합니다. API Gateway에는 최소 요금이나 시작 비용이 없습니다. 수신한 API 호출과 전송된 데이터 양에 대해서만 비용을 지불하며, API Gateway 계층형 요금 모델을 사용하면 API 사용량이 확장됨에 따라 비용을 절감할 수 있습니다. 자세한 내용은 [Amazon API Gateway](#)를 참조하세요.

FAQ: AMS의 API Gateway

Q: AMS 계정에서 Amazon API Gateway에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct)

변경 유형을 사용하여 RFC를 제출하여 API Gateway에 대한 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다.

다customer_apigateway_author_rolecustomer_apigateway_cloudwatch_role. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon API Gateway를 사용할 때 제한 사항은 무엇인가요?

- API Gateway 구성은 AMS 인프라에 대한 수정을 방지하기 위해 AMS- 또는 MC- 접두사가 없는 리소스로 제한됩니다.
- CREATE Elastic Load Balancer의 무단 생성을 방지하기 위해 VPCLink에 대한 권한이 비활성화됩니다. VPCLinks 필요한 경우 [Application Load Balancer | 생성](#)을 참조하세요.

Q: AMS 계정에서 Amazon API Gateway를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

배포하려는 API Gateway 유형에 따라 다릅니다. 독립 실행형 서비스일 수도 있지만 기존 서비스(예: 네트워크 로드 밸런서)에 대한 액세스를 요청할 수도 있습니다.

AMS SSP를 사용하여 AMS 계정에서 Alexa for Business 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Alexa for Business 기능에 직접 액세스할 수 있습니다. Alexa for Business는 조직과 직원이 Alexa를 사용하여 더 많은 작업을 수행할 수 있는 서비스입니다. Alexa for Business를 사용하면 Alexa를 지능형 어시스턴트로 사용하여 회의실, 책상, 심지어 집이나 이동 중에 이미 사용 중인 Alexa 디바이스에서도 생산성을 높일 수 있습니다. IT 및 시설 관리자는 Alexa for Business를 사용하여 직장 내 기존 회의실의 사용률을 측정하고 늘릴 수 있습니다.

자세한 내용은 [Alexa for Business](#)를 참조하세요.

AWS Managed Services의 Alexa for Business FAQ

Q: AMS 계정에서 Alexa for Business에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다: `customer_alex_console_role`. Alexa for Business에서 제공하는 디바이스 설정 도구에 대한 `customer_alex_device_setup_user`도 생성됩니다. 그러면이 디바이스 설정 도구를 사용하여 디바이스를 설정할 수 있습니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Alexa for Business 게이트웨이를 사용하면 Alexa for Business를 Cisco Webex 및 Poly Group Series 엔드포인트에 연결하여 음성으로 회의를 제어할 수 있습니다. 게이트웨이 소프트웨어는 온프레미스 하드웨어에서 실행되며 Alexa for Business에서 Cisco 엔드포인트로 회의 지시문을 안전하게 프록시합니다. 게이트웨이가 Alexa for Business와 통신하려면 두 쌍의 AWS 자격 증명이 필요합니다. 제한된 액세스 IAM 사용자 2개를 제공합니다. `customer_alex_gateway_installer_user` Alexa for Business 게이트웨이 `customer_alex_gateway_execution_user`의 경우 게이트웨이를 설치하기 위한 IAM 사용자와 게이트웨이를 작동하기 위한 IAM 사용자 1개를 제공합니다. 이들은 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 개체 또는 정책 생성(검토 필요) 변경 유형 (ct-3dpd8mdd9jn1r)이 포함된 RFC를 제출하여 요청할 수 있습니다.

Note

사용 보고서를 생성하여 Amazon S3로 보내려면 자체 프로비저닝된 서비스 RFC에 Amazon S3 버킷 이름을 지정합니다.

Q: AMS 계정에서 Alexa for Business를 사용할 때 적용되는 제한 사항은 무엇인가요?

제한은 없습니다. Alexa for Business의 전체 기능은 Alexa for Business 자체 프로비저닝 서비스 역할에서 사용할 수 있습니다.

Q: AMS 계정에서 Alexa for Business를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- WPA2 Enterprise Wi-Fi를 사용하여 공유 디바이스를 설정하려는 경우 AWS Private Certificate Authority가 필요한 디바이스 설정 도구에서이 네트워크 보안 유형을 지정합니다.
- AMS는 네임스페이스 "A4B"로 시작하는 보안 키만 생성합니다. 이는이 네임스페이스에만 제한됩니다.

Q: Alexa for Business 기능에는 별도의 RFCs 필요합니까?

Alexa Voice Service(AVS) 디바이스를 Alexa for Business에 등록하려면 Alexa 내장 디바이스 메이커에 대한 액세스를 제공합니다. 이렇게 하려면 Alexa for Business 콘솔에서 관리 | 기타 | 기타 변경 유형을 사용하여 배포할 수 있는 IAM 역할을 생성해야 합니다. 이를 통해 AVS 디바이스 제조업체는 사용자를 대신하여 Alexa for Business에 디바이스를 등록하고 관리할 수 있습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon AppStream 2.0 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon AppStream 2.0(AppStream 2.0) 기능에 직접 액세스할 수 있습니다. AppStream 2.0을 사용하면 데스크톱 애플리케이션을 다시 작성 AWS하지 않고도 로 이동할 수 있습니다. AppStream 2.0에 애플리케이션을 설치하고, 시작 구성을 설정하고, 사용자가 애플리케이션을 사용할 수 있도록 할 수 있습니다. AppStream 2.0은 다양한 가상 머신 옵션을 제공하므로 애플리케이션 요구 사항에 가장 적합한 인스턴스 유형을 선택하고 자동 크기 조정 파라미터를 설정하여 최종 사용자의 요구 사항을 쉽게 충족할 수 있습니다. AppStream 2.0을 사용하면 자체 네트워크에서 애플리케이션을 시작할 수 있습니다. 즉, 애플리케이션이 기존 AWS 리소스와 상호 작용할 수 있습니다.

Amazon AppStream 2.0을 사용하면 이미지 빌더를 사용하여 애플리케이션을 빠르고 쉽게 설치, 테스트 및 업데이트할 수 있습니다. Microsoft Windows Server 2012 R2, Windows Server 2016 또는 Windows Server 2019에서 실행되는 모든 애플리케이션이 지원되므로 수정할 필요가 없습니다. 테스트가 완료되면 애플리케이션 시작 구성, 기본 사용자 설정을 설정하고 사용자가 액세스할 수 있도록 이미지를 게시할 수 있습니다.

자세한 내용은 [AppStream 2.0](#)을 참조하세요.

AWS Managed Services FAQ의 AppStream 2.0

Q: AMS 계정에서 AppStream 2.0에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출하여 AppStream 2.0에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_appstream_console_role.

또한 customer_appstream_stream_role는 Active Directory 로그인 자격 증명을 사용하여 사용자를 인증해야 하는 애플리케이션을 스트리밍하도록 배포됩니다.

계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 AppStream 2.0을 사용할 때 제한 사항은 무엇인가요?

- 다음 기능은 AMS Support 팀에서 구성해야 하며 특정 RFCs 필요합니다. 추가 기능 요청에 대한 지침은 섹션 4에서 확인할 수 있습니다.
 - 인터페이스 VPC 엔드포인트에서 생성 및 스트리밍.
 - 프라이빗 네트워크에서 홈 폴더 및 애플리케이션 설정 지속성을 위한 Amazon S3 엔드포인트를 지원합니다.
 - 모든 플릿 스트리밍 인스턴스에서 사용할 수 있는 IAM 역할을 생성하고 선택합니다.
 - AppStream 2.0 플릿 및 이미지 빌더 Microsoft Active Directory 도메인 조인.
 - AppStream 2.0 사용자 지정 사용 보고서 생성.
 - 사용자 지정 브랜딩은 현재 지원되지 않습니다.

Q: AMS 계정에서 AppStream 2.0을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AppStream 2.0을 온보딩하기 위해 RFC를 제출하는 동안 AppStream 2.0 사용 보고서에 사용할 Amazon S3 버킷 이름을 포함합니다. AppStream 2.0이 온보딩 customer-appstream-usagereports-policy될 때 생성되는 버킷 이름이 추가됩니다.

Q: 별도의 RFCs 필요한 AppStream 2.0 기능은 무엇입니까?

- AppStream 2.0용 인터페이스 VPC 엔드포인트를 선택하려면 관리 | 기타 | 기타 | 업데이트 변경 유형 RFC를 제출하여 계정에 VPC 엔드포인트를 생성합니다. AppStream 2.0용 사용자 지정 엔드포인트를 생성하는 단계는 AppStream 2.0 사용 설명서의 [인터페이스 VPC 엔드포인트에서 생성 및 스트리밍을 참조하세요](#).
- 관리 | 기타 | 기타 | 변경 유형 생성 RFC를 사용하여 Amazon S3 VPC 엔드포인트를 요청하여 프라이빗 네트워크에서 홈 폴더 및 애플리케이션 설정 지속성에 대한 Amazon S3 엔드포인트 지원을 구성할 수 있습니다. RFC에는 홈 폴더 콘텐츠를 호스팅하는 대상 Amazon S3 버킷 또는 애플리케이션 설정 Amazon S3 버킷이 각각 포함되어야 합니다. 이 RFC는 Amazon S3 VPC 엔드포인트에 액세스하는 데 필요한 권한을 AppStream 2.0에 제공합니다. 스트림에 대한 사용자 지정 엔드포인트를 생성

하는 단계는 AppStream 2.0 사용 설명서의 [홈 폴더에 Amazon S3 VPC 엔드포인트 사용 및 애플리케이션 설정 지속성](#)을 참조하세요.

- 모든 플릿 스트리밍 인스턴스에서 사용할 수 있는 IAM 역할을 생성하고 선택하려면 필요한 정책을 사용하여 IAM 역할을 요청하는 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 개체 또는 정책 생성(검토 필요) 변경 유형(ct-3dpg8mdd9jn1r) RFC를 제출합니다. IAM 역할 이름은 항상 접두사 "customer_appstream"으로 시작해야 합니다.
- Amazon AppStream 2.0 플릿 및 이미지 빌더는 Active Directory(AD)에서 서비스 계정 생성을 위한 관리 | 기타 | 기타 | 업데이트 변경 유형 RFC를 제출하여 Microsoft Active Directory의 도메인에 조인할 수 있습니다. Microsoft Active Directory에 조인하는 데 필요한 최소 권한은 AppStream 2.0 설명서의 [Active Directory 컴퓨터 객체를 생성하고 관리할 수 있는 권한 부여에 정의되어 있습니다](#).
- 사용자 지정 AppStream 2.0 사용 보고서를 생성하려면 다음을 요청하는 관리 | 기타 | 기타 | 변경 유형 생성 RFC를 제출합니다.
 - "AppStreamUsageReports" CFN 스택 생성
 - 계정에서 "customer_appstream_usagereports_role" 프로비저닝
 - 또한 다음 세부 정보를 제공합니다.
 - CRON 표현식을 제공하여 크롤러 실행을 예약합니다. 기본적으로 매일 23:00 UTC입니다.
 - Athena 쿼리 결과에 사용할 Amazon S3 버킷 ARN입니다. 이 버킷에는 접두사가 있어야 합니다. aws-athena-query-results
 - AppStream 2.0 사용 보고서 로그용 Amazon S3 버킷 ARN.

역할이 프로비저닝된 후 역할을 페더레이션 솔루션에 온보딩하고 로그인한 다음 사용 보고서 역할을 사용하여 사용자 지정 보고서를 생성하기 위해 AWS GlueAWS Glue 및 Athena에 액세스합니다. AppStream 2.0 사용 보고서 사용에 대한 자세한 내용은 [AppStream 2.0 설명서의 사용자 지정 보고서 생성 및 AppStream 2.0 사용 데이터 분석](#)을 참조하세요. AppStream

AMS SSP를 사용하여 AMS 계정에서 Amazon Athena 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Athena(Athena) 기능에 직접 액세스할 수 있습니다. Athena는 표준 SQL을 사용하여 Amazon S3의 데이터를 분석하는데 도움이 되는 대화형 쿼리 서비스입니다. Athena는 서버리스 서비스이므로 관리할 인프라가 없으며 실행한 쿼리에 대해서만 비용을 지불하면 됩니다. Amazon S3의 데이터를 가리키고 스키마를 정의한 다음 표준 SQL을 사용하여 쿼리를 시작합니다. 대부분의 결과는 몇 초 내에 전달됩니다. Athena를 사용하면 분석을 위해 데이터를 준비하는 데 복잡한 ETL(추extract-transform-load) 작업이 필요하지 않습니다. 따라서 SQL 기술을 보유한 모든 사용자가 대규모 데이터 세트를 빠르게 분석할 수 있습니다. 자세한 내용은 [Amazon Athena](#)를 참조하세요.

FAQ: AMS의 Athena

Q: AMS 계정에서 Amazon Athena에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Athena에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_athena_console_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Athena를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Athena의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Athena를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Athena는 로 생성된 데이터 카탈로그/메타스토어를 사용하므로 AWS Glue 서비스에 대한 주요 종속성이 있습니다 AWS Glue. 따라서 AWS Glue 권한은 성공적인 Athena RFC에 포함됩니다.

역할에는 Amazon S3 버킷 customer_athena_console_role에 대한 사전 조건이 있습니다. 새 버킷을 생성하려면 자동 CT ct-1a68ck03fn98r(배포 | 고급 스택 구성 요소 | S3 스토리지 | 생성)를 사용합니다. 이 자동 CT를 사용하여 Athena용 S3 버킷을 생성하는 경우 버킷 이름은 접두사 로 시작해야 합니다 athena-query-results-*.

AMS SSP를 사용하여 AMS 계정에서 Amazon Bedrock 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Bedrock 기능에 직접 액세스할 수 있습니다. Amazon Bedrock은 선도적인 AI 스타트업에서 고성능 파운데이션 모델(FMs)을 만들고 통합 API를 통해 사용할 AWS 수 있는 완전관리형 서비스입니다. 다양한 파운데이션 모델 중에서 선택하여 사용 사례에 가장 적합한 모델을 찾을 수 있습니다. 또한 Amazon Bedrock은 보안, 프라이버시 및 책임감 있는 AI를 갖춘 생성형 AI 애플리케이션을 구축할 수 있는 다양한 기능을 제공합니다. Amazon Bedrock을 사용하면 사용 사례에 맞는 최고 수준의 파운데이션 모델을 쉽게 실험 및 평가하고, 미세 조정 및 검색 증강 생성(RAG)과 같은 기술로 데이터를 사용하여 프라이빗으로 사용자 지정하고, 엔터프라이즈 시스템 및 데이터 소스를 사용하여 작업을 실행하는 에이전트를 구축할 수 있습니다.

Amazon Bedrock의 서버리스 환경을 사용하면 인프라를 관리할 필요 없이 AWS 도구를 사용하여 파운데이션 모델을 빠르고 비공개로 사용자 지정하고 애플리케이션을 쉽고 안전하게 통합 및 배포할 수 있습니다. 자세한 내용은 [Amazon Bedrock](#)을 참조하세요.

FAQ: AMS의 Amazon Bedrock

Q: AMS 계정에서 Amazon Bedrock에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Amazon Bedrock에 대한 액세스를 요청하려면 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_bedrock_console_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Bedrock을 사용할 때 제한 사항은 무엇인가요?

- Amazon Bedrock 지식 기반은 현재 AMS에서 지원되지 않는 Amazon OpenSearch Service Serverless에 대한 종속성으로 인해 SSPS 역할의 일부로 기본적으로 지원되지 않습니다.
- Bedrock Studio는 Amazon DataZone과 같은 지원되지 않는 서비스에 종속되어 있으므로 지원되지 않습니다.

Q: AMS 계정에서 Amazon Bedrock을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- AWS Marketplace 권한이 필요한 타사 모델 구독은 기본 역할 (AWSManagedServicesAdminRoleMALZ의 경우, SALZCustomer_ReadOnly_Role의 경우)로 수행해야 합니다. 이는 기본 역할에 AWS Marketplace 권한이 포함되기 때문입니다.
- 데이터 암호화를 사용하는 경우 콘솔 역할 생성을 요청할 때 AWS KMS 키 ARN을 제공해야 합니다. 또한 사용 중인 Amazon S3 버킷의 이름에 "bedrock"이 있어야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon CloudSearch 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon CloudSearch 기능에 직접 액세스할 수 있습니다. Amazon CloudSearch는 웹 사이트 또는 애플리케이션에 대한 검색 솔루션을 비용 효율적으로 설정, 관리 및 확장하는 데 사용하는 AWS 클라우드의 관리형 서비스입니다. Amazon CloudSearch는 강조 표시, 자동 완성 및 지리 공간 검색과 같은 34개 언어와 인기 있는 검색 기능을 지원합니다. 자세한 내용은 [Amazon CloudSearch](#)를 참조하세요.

Note

AWS는 2024년 7월 25일부터 Amazon CloudSearch에 대한 새로운 고객 액세스를 종료했습니다. Amazon CloudSearch 기존 고객은 서비스를 정상적으로 계속 사용할 수 있습니다. AWS는 계속해서 Amazon CloudSearch의 보안, 가용성 및 성능 개선에 투자하지만 새로운 기능을 도입할 계획은 없습니다.

Amazon CloudSearch와 Amazon OpenSearch Service의 차이점과 OpenSearch Service로 전환하는 방법을 이해하려면 클라우드 아키텍트(CA)에 문의하여 지침을 받으세요. OpenSearch Service로 전환하는 방법에 대한 자세한 내용은 [Amazon CloudSearch에서 Amazon OpenSearch Service 서비스로 전환을 참조하세요](#).

AWS Managed Services의 Amazon CloudSearch FAQ

Q: AMS 계정에서 Amazon CloudSearch에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon CloudSearch에 대한 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다 customer_csearch_admin_role customer_csearch_dev_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon CloudSearch를 사용할 때 제한 사항은 무엇인가요?

Amazon CloudSearch의 전체 기능은 AMS 계정에서 사용할 수 있습니다. 모든 AMS 지원 데이터베이스 솔루션은 현재 Amazon CloudSearch에서 지원됩니다. 현재 DynamoDB는 인덱싱할 수 없는 유일한 관리형 AWS 데이터베이스 솔루션입니다.

Q: AMS 계정에서 Amazon CloudSearch를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon CloudSearch는 Amazon S3가 자격 증명 공급자와 협력하여 입력 데이터를 자동으로 분석하고 테이블 필드를 결정하는 데 의존합니다. Amazon S3에 대한 액세스는 이 RFC와 함께 제공되지 않으므로 서비스 요청에서 별도로 요청해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon CloudWatch Synthetics 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Amazon CloudWatch Synthetics 기능에 액세스할 수 있습니다. Amazon CloudWatch Synthetics를 사용하여 'canary'를 생성하여 엔드포인트와 APIs 모니터링할 수 있습니다.

canary는 일정에 따라 실행되는 Node.js 또는 Python으로 작성된 구성 가능한 스크립트입니다. Node.js 또는 Python을 프레임워크로 사용하는 Lambda 함수를 계정에 생성합니다. canary는 HTTP 프로토콜과 HTTPS 프로토콜 모두에서 작동합니다. 카나리아는 엔드포인트의 가용성과 지연 시간을 확인하고 로드 시간 데이터와 UI 스크린샷을 저장할 수 있습니다. REST API, URL 및 웹사이트 콘텐츠

를 모니터링하고 피싱, 코드 주입 및 교차 사이트 스크립팅으로 인한 무단 변경 사항을 검사할 수 있습니다.

카나리아는 고객과 동일한 경로를 따르고 동일한 작업을 수행하므로 애플리케이션에 고객 트래픽이 없는 경우에도 고객 경험을 지속적으로 확인할 수 있습니다. 카나리를 사용하면 고객보다 먼저 문제를 발견할 수 있습니다. 자세한 내용은 [Amazon CloudWatch: 합성 모니터링 사용](#)을 참조하세요.

AWS Managed Services FAQ의 Amazon CloudWatch Synthetics

Q: AMS 계정에서 Amazon CloudWatch Synthetics에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon CloudWatch Synthetics에 대한 액세스를 요청합니다. 이 RFC는 계정에 'customer_cw_synthetics_console_role' 및 'customer_cw_synthetics_canary_lambda_role'이라는 IAM 역할을 프로비저닝합니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 'customer_cw_synthetics_console_role' 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon CloudWatch Synthetics를 사용할 때 적용되는 제한 사항은 무엇인가요?

AMS 계정에서 Amazon CloudWatch Synthetics를 사용하는 데는 제한이 없습니다. AMS 제공 서비스 역할 'customer_cw_synthetics_canary_lambda_role' 외부에서 canary에 대한 역할을 생성하는 것은 금지됩니다.

Q: AMS 계정에서 Amazon CloudWatch Synthetics를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

카나리아는 기본 Amazon CloudWatch Synthetics S3 버킷을 생성하고 사용합니다. "cw-syn-results-*accountnumber*-*default-region*"

AMS SSP를 사용하여 AMS 계정에서 Amazon Cognito 사용자 풀 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Cognito 사용자 풀 기능에 직접 액세스할 수 있습니다. Amazon Cognito 사용자 풀은 수억 명의 사용자로 확장되는 안전한 사용자 디렉터리를 제공합니다. 완전 관리형 서비스인 Amazon Cognito 사용자 풀은 서버 인프라 구축에 대한 걱정 없이 설정할 수 있습니다. 이 서비스를 사용하면 내부 애플리케이션과 통합하는데 사용할 수 있는 최종 사용자 풀을 관리할 수 있습니다. 이 서비스는 웹 또는 모바일 애플리케이션을 위한 사용자 지정 데이터베이스 또는 최종 사용자 디렉터리의 대안을 제공합니다. 동시에 Amazon Cognito 사용자 풀은 암호 정책, 다중 인증, 암호 복구 및 서비스 자체 가입과 같은 디렉터리 서비스의

전체 기능 세트를 제공합니다. 또한 애플리케이션이 OpenID, Facebook, Amazon 또는 Google과 같은 다른 인기 있는 퍼블릭 서비스에서 액세스를 페더레이션할 수 있습니다.

Amazon Cognito는 두 가지 주요 제품으로 나뉩니다. Amazon Cognito 사용자 풀 및 Amazon Cognito 자격 증명 공급자. 이 섹션에서는 Amazon S3 또는 DynamoDB와 같은 다른 서비스에 대한 액세스를 제공하는 Amazon Cognito 사용자 풀에 중점을 둡니다. AWS Amazon S3 DynamoDB 이 서비스를 사용하면 Amazon Cognito 사용자 풀 또는 타사 자격 증명 공급자를 사용하여 AWS 서비스에 대한 액세스를 제공할 수 있습니다. 또한 익명 게스트 액세스를 사용하여 AWS 서비스에 대한 액세스를 제공합니다. Amazon Cognito 사용자 풀의 강력한 특성으로 인해 계정의 잠재적 보안 중단을 방지하기 위해 운영 수동 서비스로 case-by-case 수동으로 관리됩니다. 자세한 내용은 [Amazon Cognito 사용자 풀을 참조하세요](#).

AWS Managed Services FAQ의 Amazon Cognito 사용자 풀

일반적인 질문과 답변:

Q: AMS 계정의 Amazon Cognito 사용자 풀에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AMS에서 Amazon Cognito 사용자 풀의 구현은 2단계 프로세스입니다.

1. 관리 제출 | 기타 | 기타 | (ct-1e1xtak34nx76) 변경 유형을 생성하고 AMS 계정에서 Amazon Cognito 사용자 풀 생성을 요청합니다. 다음 정보를 포함합니다.
 - AWS 리전.
 - Cognito 사용자 풀의 이름입니다.
 - Amazon Simple Email Service(Amazon SES)를 사용하여 기본 내부 Cognito 메일 서비스 대신 메시지 및 알림을 보내려는 경우 고객은 계정에서 Amazon SES Service에 대해 이미 검증된 이메일 주소를 제공해야 합니다. 이 주소는 메시지의 "From" 및 "REPLY-TO" 필드에 사용됩니다. 또한 Amazon SES가 활성화된 리전(us-east-1, eu-west-1 또는 us-west-2)을 표시해야 합니다.
 - 가 일회용 암호 및 확인에 SMS 메시지를 사용하려는 경우 고객은 이를 표시해야 합니다.
2. 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 사용자 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다 customer_cognito_admin_rolecustomer_cognito_importjob_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다. 이러한 역할을 사용하면 Amazon Cognito 사용자 풀을 관리하고, 풀에서 사용자 및 그룹을 관리하고, 사용자를 위한 가져오기 작업을 생성하고, 알림 및 구독 메시지를 수정하고, 애플리케이션을 사용자 풀에 연결하고, 풀에 페더레이션 서비스를 추가하고, 이미 생성된 풀을 삭제할 수 있습니다.

Q: AMS 계정의 Amazon Cognito 사용자 풀 사용에 대한 제한 사항은 무엇인가요?

Amazon Cognito 사용자 풀을 생성할 수 없습니다. 이 작업을 수행하려면 Amazon SES 및 Amazon Simple Notification Service(SNS)와 같이 Amazon Cognito에서 사용하는 서비스를 활용하기 위한 IAM 역할을 생성해야 합니다. Amazon SNS

Q: AMS 계정에서 Amazon Cognito 사용자 풀을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon SES를 사용하여 사용자 풀에 이메일로 메시지와 알림을 보내려면 계정에서 Amazon SES 서비스를 이미 활성화하고 전송된 이메일의 "FROM" 및 "REPLY-TO" 필드에 사용해야 하는 이메일 주소를 이미 검증해야 합니다. Amazon SES를 사용하여 이메일 주소를 검증하는 방법에 대한 자세한 내용은 [Amazon SES에서 이메일 주소 확인을 참조하세요](#).

AMS SSP를 사용하여 AMS 계정에서 Amazon Comprehend 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Comprehend 기능에 직접 액세스할 수 있습니다. Amazon Comprehend는 기계 학습을 사용하여 텍스트에서 인사이트와 관계를 찾는 자연어 처리(NLP) 서비스이므로 기계 학습 경험이 필요하지 않습니다. Amazon Comprehend는 기계 학습을 사용하여 비정형 데이터의 인사이트와 관계를 발견하는 데 도움이 됩니다. 이 서비스는 텍스트의 언어를 식별하고, 주요 문구, 장소, 사람, 브랜드 또는 이벤트를 추출하고, 텍스트가 얼마나 긍정적이거나 부정적인지 이해하고, 토큰화 및 음성 부분을 사용하여 텍스트를 분석하고, 주제별로 텍스트 파일 모음을 자동으로 구성합니다. Amazon Comprehend에서 AutoML 기능을 사용하여 조직의 요구 사항에 맞게 고유하게 조정된 사용자 지정 엔터티 또는 텍스트 분류 모델 세트를 구축할 수도 있습니다. 자세한 내용은 [Amazon Comprehend](#)를 참조하세요.

AWS Managed Services FAQ의 Amazon Comprehend

Q: AMS 계정에서 Amazon Comprehend에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Amazon Comprehend 콘솔 및 데이터 액세스 역할은 두 개의 AMS Service RFCs.

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_comprehend_console_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Comprehend를 사용할 때 제한 사항은 무엇인가요?

Amazon Comprehend 콘솔을 통한 새 IAM 역할 생성 기능은 제한됩니다. 그렇지 않으면 AMS 계정에서 Amazon Comprehend의 전체 기능을 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Comprehend를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon S3 버킷이 AWS KMS 키로 암호화된 경우 Amazon Comprehend를 사용하려면 Amazon S3 및 AWS Key Management Service (AWS KMS)가 필요합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Connect 프로비저닝

Note

신중한 고려 후 2026년 5월 20일부터 Amazon Connect Voice ID에 대한 지원을 종료하기로 결정했습니다. Amazon Connect Voice ID는 2025년 5월 20일부터 더 이상 신규 고객을 받지 않습니다. 2025년 5월 20일 이전에 서비스에 가입한 계정이 있는 기존 고객은 Amazon Connect Voice ID 기능을 계속 사용할 수 있습니다. 2026년 5월 20일 이후에는 Amazon Connect Voice ID를 더 이상 사용할 수 없습니다.

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Connect 기능에 직접 액세스할 수 있습니다. Amazon Connect는 기업이 더 저렴한 비용으로 우수한 고객 서비스를 제공할 수 있도록 지원하는 옴니채널 클라우드 고객 센터입니다. Amazon Connect는 고객과 에이전트에게 음성 및 채팅 전반에 걸쳐 원활한 경험을 제공합니다. 여기에는 기술 기반 라우팅, 강력한 실시간 및 기록 분석, easy-to-use 직관적인 관리 도구를 위한 하나의 도구 세트가 포함되며, 모두 pay-as-you-go 요금이 적용됩니다.

AMS 다중 계정 랜딩 존 또는 단일 계정 랜딩 존 계정에서 가상 고객 센터 인스턴스의 인스턴스를 하나 이상 생성할 수 있습니다. 에이전트 액세스에 기존 SAML 2.0 자격 증명 공급자를 사용하거나 사용자 수명 주기 관리에 Amazon Connect 네이티브 지원을 사용할 수 있습니다.

또한 Amazon Connect 콘솔에서 각 Amazon Connect 인스턴스의 수신자 부담/직통 전화번호를 신청할 수 있습니다. easy-to-use 그래픽 사용자 인터페이스를 사용하여 풍부한 고객 응대 흐름을 생성하여 원하는 고객 경험과 라우팅을 달성할 수 있습니다. 고객 응대 흐름은 AWS Lambda 함수를 활용하여 온프레미스 데이터 스토어 및 API와 통합할 수 있습니다. Kinesis Streams 및 Firehose를 사용하여 데이터 스트리밍을 활성화할 수도 있습니다.

통화 녹음, 채팅 기록 및 보고서는 AWS KMS 키를 사용하여 암호화된 Amazon S3 버킷에 저장됩니다. 고객 응대 흐름 로그는 CloudWatch 로그 그룹에 저장할 수 있습니다.

자세한 내용은 [Amazon Connect](#)를 참조하세요.

AWS Managed Services의 Amazon Connect FAQ

Q: AMS 계정에서 Amazon Connect에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다 customer_connect_console_rolecustomer_connect_user_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Connect를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Connect의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Connect를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- 표준 AMS RFCs를 사용하여 AWS KMS 키와 Amazon S3 버킷을 생성해야 합니다. 통화 녹음 및 채팅 기록을 저장하려면 Amazon S3 버킷이 필요합니다.
- Active Directory(AD)와 통합하려면 AMS 호스팅 Amazon Connect 인스턴스와 온프레미스 디렉터리 서비스 간의 통합에 AD 커넥터가 필요합니다. AD 커넥터는 '관리 | 기타 | 기타' RFC를 요청하여 계정에서 구성할 수 있습니다.
- 고객 응대 흐름 요구 사항에 따라 다음과 같은 선택적 자체 프로비저닝 서비스를 활성화할 수 있습니다.
 - AWS Lambda: Lambda 함수를 사용하여 고객 응대 흐름을 확장하여 기존 온프레미스 데이터 스토어 또는 APIs. Lambda 자체 프로비저닝 서비스를 사용하여 Lambda 함수를 생성할 수 있습니다.
 - Amazon Kinesis Data Streams: 데이터 스트림을 생성하여 외부 애플리케이션으로의 데이터 스트리밍을 활성화할 수 있습니다. 고객 응대 추적 레코드 또는 에이전트 이벤트를 스트리밍할 수 있습니다.
 - Amazon Kinesis Data Firehose: Data Firehose를 생성하여 대용량 고객 응대 추적 레코드를 외부 애플리케이션으로 스트리밍할 수 있습니다.
 - Amazon Lex: Amazon Lex Chatbots를 활용하여 풍부한 고객 경험과 자동화를 위해 Amazon Alexa 서비스를 활용하는 스마트 고객 응대 흐름을 생성할 수 있습니다.
- Q: 아웃바운드 또는 인바운드 통화에 대한 국가 목록을 추가하도록 요청하려면 어떻게 해야 하나요?

아웃바운드 또는 인바운드 통화 국가 목록을 추가하려면 AMS에 서비스 요청을 제출합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Data Firehose 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Data Firehose 기능에 직접 액세스할 수 있습니다. Firehose는 스트리밍 데이터를 데이터 레이크, 데이터 스토어 및 분석 도구로 안정적으로 로드하는 가장 쉬운 방법입니다. 스트리밍 데이터를 캡처하고 변환하여 Amazon

S3, Amazon Redshift, Amazon OpenSearch Service 및 [Splunk](#)로 로드할 수 있으므로 현재 이미 사용 중인 기존 비즈니스 인텔리전스 도구 및 대시보드를 사용하여 거의 실시간으로 분석할 수 있습니다. 데이터 처리량에 맞게 자동으로 확장되며 지속적인 관리가 필요하지 않은 완전 관리형 서비스입니다. 또한 데이터를 로드하기 전에 배치, 압축, 변환 및 암호화하여 대상에서 사용되는 스토리지 양을 최소화하고 보안을 강화할 수 있습니다. 자세한 내용은 [Amazon Data Firehose란 무엇입니까?](#)를 참조하세요.

AWS Managed Services FAQ의 Firehose

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Data Firehose에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_kinesis_firehose_user_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Firehose를 사용할 때 적용되는 제한 사항은 무엇입니까?

제한은 없습니다. Amazon Data Firehose의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Firehose를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

각 전송 스트림에 대해 새 서비스 연결 IAM 역할을 요청해야 합니다. 역할 정책을 필요한 리소스 권한(S3 버킷/KMS 키/Lambda 함수/Kinesis 스트림 포함)으로 업데이트하여 모든 스트림에 대해 단일 서비스 연결 역할을 재사용할 수도 있습니다.

Firehose를 추가하기 위해 RFC를 제출하면 AMS 운영 엔지니어가 Data Firehose와 연결하려는 리소스의 ARNs(예: S3 AWS KMS, Lambda 및 Kinesis Streams)에 대한 서비스 요청을 통해 연락을 드릴 것입니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon DevOpsGuru 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon DevOpsGuru 기능에 직접 액세스할 수 있습니다. Amazon DevOpsGuru는 개발자와 운영자가 애플리케이션의 성능과 가용성을 쉽게 개선할 수 있는 완전관리형 운영 서비스입니다. DevOps Guru는 운영 문제 식별과 관련된 관리 작업을 없애므로 애플리케이션을 개선하기 위한 권장 사항을 신속하게 구현할 수 있습니다. 이제 DevOps Guru는 애플리케이션을 개선하는 데 사용할 수 있는 사후 대응 인사이트를 제공합니다. 또한 향후 애플리케이션에 영향을 미칠 수 있는 운영 문제를 방지하는 데 도움이 되는 사전 예방 인사이트를 제공합니다. DevOps Guru는 운영 데이터, 애플리케이션 지표 및 이벤트를 분석하여 정상적인 운영 패턴에서 벗어나는 동작을 식별하기 위해 기계 학습을 적용합니다. DevOps Guru가 운영 문제 또는

위험을 감지하면 알림이 전송됩니다. DevOps Guru는 현재 및 향후 예상되는 운영 문제를 해결하기 위해 각 문제에 대한 지능적인 권장 사항을 제시합니다.

자세한 내용은 [Amazon DevOpsGuru란 무엇입니까?](#)를 참조하세요.

AWS Managed Services FAQ의 Amazon DevOpsGuru

Q: AMS 계정에서 Amazon DevOpsGuru에 대한 액세스를 요청하려면 어떻게 해야 하나요?

액세스를 요청하려면 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_devopsguru_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon DevOpsGuru를 사용하는 데 따르는 제한 사항은 무엇인가요?

제한은 없습니다. Amazon DevOpsGuru의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon DevOpsGuru를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

사전 조건은 없습니다. DevOpsGuru는 Amazon CloudWatch Logs, RDS Insights AWS X-Ray AWS Lambda 및 AWS 서비스를 활용합니다 AWS CloudTrail.

AMS SSP를 사용하여 AMS 계정에서 Amazon DocumentDB(MongoDB 호환) 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon DocumentDB(MongoDB 호환) 기능에 직접 액세스할 수 있습니다. Amazon DocumentDB(MongoDB 호환)는 MongoDB 워크로드를 지원하는 빠르고 확장 가능하며 가용성이 높고 완전 관리형 문서 데이터베이스 서비스입니다. Amazon DocumentDB는 미션 크리티컬 MongoDB 워크로드를 대규모로 운영할 때 필요한 성능, 확장성 및 가용성을 제공합니다. Amazon DocumentDB는 MongoDB 클라이언트가 MongoDB 서버에서 기대하는 응답을 에뮬레이션하여 Apache 2.0 오픈 소스 MongoDB 3.6 API를 구현하므로 Amazon DocumentDB에서 기존 MongoDB 드라이버 및 도구를 사용할 수 있습니다. Amazon DocumentDB에서는 스토리지와 컴퓨팅이 분리되어 각 스토리지와 컴퓨팅을 독립적으로 확장할 수 있으며, 데이터 크기에 관계없이 지연 시간이 짧은 읽기 전용 복제본을 최대 15개까지 추가하여 초당 수백만 개의 요청으로 읽기 용량을 늘릴 수 있습니다. Amazon DocumentDB는 99.99% 가용성을 위해 설계되었으며 3개의 AWS 가용 영역(AZs. AWS Database Migration Service (DMS)를 무료로(6개월 동안) 사용하여 가동 중지 없이 온프레미스 또는 Amazon Elastic Compute Cloud(Amazon EC2) MongoDB 데이터베이스를 Amazon DocumentDB로 마이그레이션할 수 있습니다. 자세한 내용은 [Amazon DocumentDB\(MongoDB 호환\)를 참조하세요.](#)

AWS Managed Services Amazon DocumentDB FAQ

Q: AMS 계정에서 Amazon DocumentDB에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Amazon DocumentDB 콘솔 및 데이터 액세스 역할은 두 개의 AMS RFCs

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon DocumentDB에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_documentdb_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon DocumentDB를 사용할 때 제한 사항은 무엇인가요?

Amazon DocumentDB에는 Amazon RDS 관련 권한이 필요합니다. AMS는 Amazon RDS를 완전히 관리하므로 Amazon DocumentDB의 IAM 역할에는 Amazon RDS의 작업에 대한 몇 가지 제한이 포함됩니다. 다음과 같은 제한 사항이 있습니다.

- DeleteDBInstance 및 DeleteDBCluster APIs가 제한되었습니다. 이러한 삭제 APIs 사용하려면 관리 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 엔터티 또는 정책 업데이트 (검토 필요) 변경 유형(ct-27tuth19k52b4)을 사용하여 RFC를 제출합니다.
- Amazon RDS 인스턴스에서는 태그를 추가하거나 제거할 수 없습니다.
- Amazon DocumentDB 인스턴스는 퍼블릭으로 설정할 수 없습니다.

Q: AMS 계정에서 Amazon DocumentDB를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon S3 버킷 AWS KMS 이 AWS KMS 키로 암호화된 경우 Amazon DocumentDB를 사용하려면 Amazon S3 및가 필요합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon DynamoDB 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon DynamoDB(DynamoDB) 기능에 직접 액세스할 수 있습니다. Amazon DynamoDB는 모든 규모에서 한 자릿수 밀리초의 성능을 제공하는 키 값 및 문서 데이터베이스입니다. 인터넷 규모 애플리케이션을 위한 보안, 백업 및 복원, 인 메모리 캐싱이 내장된 완전 관리형 다중 리전 다중 활성 데이터베이스입니다. 자세한 내용은 [Amazon DynamoDB](#)를 참조하세요.

Amazon DynamoDB Accelerator(DAX)는 캐시를 DynamoDB 테이블에 추가하는 프로세스를 간소화하기 위해 설계된 라이트-스루(write-through) 캐싱 서비스입니다. DAX는 고성능 읽기가 필요한 애플리케이션을 위해 만들어졌습니다.

AWS Managed Services DynamoDB FAQ

Q: AMS 계정에서 DynamoDB 및 DAX에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | 서비스 | AWS 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 DynamoDB 및 DAX에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할 및 정책을 프로비저닝합니다.

- DynamoDB 역할 이름: `customer_dynamodb_role`
DAX 서비스 역할 이름: `customer_dax_service_role`
- DynamoDB 정책 이름: `customer_dynamodb_policy`
DAX 서비스 정책: `customer_dax_service_policy`

계정에 프로비저닝된 후에는 페더레이션 솔루션 `customer_dynamodb_role`에서 온보딩해야 합니다.

Q: AMS 계정에서 DynamoDB를 사용하는 데 따르는 제한 사항은 무엇인가요?

DynamoDB Accelerator(DAX)를 포함한 모든 DynamoDB 기능이 지원됩니다.

지정된 테이블에 대한 경보를 생성할 때 경보 이름 앞에 "customer*"를 붙여야 합니다. 예: `customer-employee-table-high-put-latency`.

DynamoDB에 대한 Amazon SNS 주제를 생성할 때 이름이 여야 합니다 `dynamodb`.

DynamoDB에서 생성한 Amazon SNS 주제를 삭제하려면 관리 | 기타 | 기타 | 변경 유형 RFC 업데이트를 제출합니다.

Q: AMS 계정에서 DynamoDB를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 DynamoDB를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Elastic Container Registry 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Elastic Container Registry(Amazon ECR) 기능에 직접 액세스할 수 있습니다. Amazon Elastic Container Registry는 개발자가 [Docker](#) 컨테이너 이미지를 쉽게 저장, 관리 및 배포할 수 있는 완전 관리형 Docker 컨테이너

레지스트리입니다. Amazon ECR은 [Amazon Elastic Container Service\(Amazon ECS\)](#)와 통합되어 프로덕션 워크플로 개발을 간소화합니다. Amazon ECR을 사용하면 자체 컨테이너 리포지토리를 운영하거나 기본 인프라를 확장할 필요가 없습니다. Amazon ECS는 가용성과 확장성이 뛰어난 아키텍처에서 이미지를 호스팅하므로 애플리케이션용 컨테이너를 안정적으로 배포할 수 있습니다. AWS Identity and Access Management (IAM)와의 통합은 각 리포지토리의 리소스 수준 제어를 제공합니다. Amazon ECR에서는 선결제 요금이나 약정이 없습니다. 리포지토리에 저장한 데이터와 인터넷으로 전송된 데이터의 양에 대해서만 비용을 지불합니다.

자세한 내용은 [Amazon Elastic Container Registry](#)를 참조하세요.

AWS Managed Services의 Amazon Elastic Container Registry FAQ

Q: AMS 계정에서 Amazon ECR에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon ECR에 대한 액세스를 요청합니다. 이 RFC는 `customer_ecr_poweruser_instance_profile_policy` 각 `customer_ecr_console_role`, 및 관련 IAM 정책, `customer_ecr_console_policy` 및 `customer_ecr_poweruser_instance_profile`와 같은 IAM 역할을 계정에 프로비저닝합니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon ECR을 사용할 때 제한 사항은 무엇인가요?

AMS 계정에서 Amazon ECR을 사용하기 위한 AMS 네임스페이스에는 제한이 있습니다. 컨테이너 이미지는 "AMS-" 또는 "Sentinel-" 접두사가 붙을 수 없습니다.

Q: AMS 계정에서 Amazon ECR을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon ECR을 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 EC2 Image Builder 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 EC2 Image Builder 기능에 직접 액세스할 수 있습니다. EC2 Image Builder는 특정 IT 표준을 충족하기 위해 소프트웨어 및 설정으로 사전 설치 및 사전 구성된 안전하고 up-to-date의 사용자 지정 "골드" 서버 이미지의 생성, 관리 및 배포를 더 쉽게 자동화할 수 있는 완전 관리형 AWS 서비스입니다.

, AWS Management Console AWS CLI 또는 APIs를 사용하여 AWS 계정에서 사용자 지정 이미지를 생성할 수 있습니다. 를 사용하면 Amazon EC2 Image Builder 마법사 AWS Management Console가 다음 단계를 안내합니다.

- 시작 아티팩트 제공
- 소프트웨어 추가 및 제거
- 설정 및 스크립트 사용자 지정
- 선택한 테스트 실행
- AWS 리전에 이미지 배포

빌드하는 이미지는 계정에 생성되며 운영 체제 패치에 대해 지속적으로 구성할 수 있습니다. 자세한 내용은 [EC2 Image Builder](#)를 참조하세요.

AWS Managed Services FAQ의 EC2 Image Builder

일반적인 질문과 답변:

Q: AMS 계정에서 EC2 Image Builder에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC를 통해 계정에 다음 IAM 역할이 프로비저닝됩니다 `customer_ec2_imagebuilder_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: EC2 Image Builder의 제한 사항은 무엇입니까?

AMS는 인프라 구성에 대한 서비스 기본값 사용을 지원하지 않습니다. 새 인프라 구성을 생성하거나 기존 인프라 구성을 사용할 수 있습니다.

AMS는 현재 컨테이너 레시피 생성을 지원하지 않습니다.

Q: EC2 Image Builder를 활성화하기 위한 사전 조건 또는 종속성은 무엇입니까?

- EC2 Image Builder 서비스 연결 역할: 서비스 연결 역할을 수동으로 생성할 필요가 없습니다. AWS Management Console, AWS CLI 또는 AWS API에서 첫 번째 Image Builder 리소스를 생성하면 Image Builder가 서비스 연결 역할을 생성합니다.
- Image Builder를 사용하여 이미지를 빌드하고 테스트를 실행하는 데 사용되는 인스턴스는 Systems Manager 서비스에 액세스할 수 있어야 합니다. SSM 에이전트가 아직 없는 경우 소스 이미지에 설치되고 이미지가 생성되기 전에 제거됩니다.
- AWS IAM: 인스턴스 프로파일과 연결하는 IAM 역할에는 이미지에 포함된 빌드 및 테스트 구성 요소를 실행할 수 있는 권한이 있어야 합니다. 인스턴스 프로파일과 연결된 IAM 역할에 `EC2InstanceProfileForImageBuilder` 및 IAM 역할 정책을 연결해야 합니다.

다AmazonSSManagedInstanceCore. IAM 역할 이름에는 *imagebuilder* 키워드가 포함되어야 합니다.

- 로깅을 구성하는 경우 인프라 구성에 지정된 인스턴스 프로파일에 대상 버킷 (arn:aws:s3:::{bucket-name}/*)에 대한 s3:PutObject 권한이 있어야 합니다. 예: JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::{bucket-name}/*"
    }
  ]
}
```

- 이름이 'imagebuilder'인 SNS 주제를 생성하여 EC2 Image Builder로부터 알림 및 알림을 받습니다.

AMS SSP를 사용하여 AMS 계정 AWS Fargate 의에서 Amazon ECS 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정의 AWS Fargate 기능에서 Amazon ECS에 직접 액세스할 수 있습니다. AWS Fargate 는 Amazon EC2 인스턴스의 Amazon EC2 에서 컨테이너를 실행하는 데 사용할 수 있는 기술입니다([의 컨테이너 AWS 참조](#)). 를 사용하면 더 이상 컨테이너를 실행하기 위해 가상 머신 클러스터를 프로비저닝, 구성 또는 확장할 필요가 AWS Fargate없습니다. 따라서 서버 유형을 선택하거나, 클러스터를 조정할 시점을 결정하거나, 클러스터 패킹을 최적화할 필요가 없습니다.

자세한 내용은 [Amazon ECS on AWS Fargate](#)을 참조하세요.

AWS Managed Services FAQ의 Fargate 기반 Amazon ECS

Q: AMS 계정에서 Fargate의 Amazon ECS에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Fargate의 Amazon ECS에 대한 액세스를 요청합니다. 이 RFC는 계정에 (ECS

정책을 연결할 기존 IAM 역할이 제공되지 않은 customer_ecs_fargate_console_role 경우), customer_ecs_fargate_events_service_role, customer_ecs_task_execution_service_role, 및 customer_ecs_codedeploy_service_role와 같은 IAM 역할을 프로비저닝합니다. AWS IAM 서비스에서 AWSServiceRoleForApplicationAutoScaling_ECSService. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Fargate에서 Amazon ECS를 사용할 때 제한 사항은 무엇인가요?

- 컨테이너 수준 활동은 하이퍼바이저 위에서 발생하며 로깅 기능은 Fargate의 Amazon ECS에 의해 제한되므로 Amazon ECS 작업 모니터링 및 로깅은 사용자의 책임으로 간주됩니다. Fargate의 Amazon ECS 사용자는 Amazon ECS 작업에 대한 로깅을 활성화하는 데 필요한 단계를 수행하는 것이 좋습니다. 자세한 내용은 [컨테이너에 대한 awslogs 로그 드라이버 활성화를 참조하세요](#).
- 컨테이너 수준의 보안 및 멀웨어 보호도 사용자의 책임으로 간주됩니다. Fargate의 Amazon ECS에는 Trend Micro 또는 사전 구성된 네트워크 보안 구성 요소가 포함되지 않습니다.
- 이 서비스는 다중 계정 랜딩 존과 단일 계정 랜딩 존 AMS 계정 모두에 사용할 수 있습니다.
- Route 53 프라이빗 호스팅 영역을 생성하려면 승격된 권한이 필요하므로 Amazon ECS [서비스 검색](#)은 기본적으로 자체 프로비저닝된 역할에서 제한됩니다. 서비스에서 서비스 검색을 활성화하려면 관리 | 기타 | 기타 | 변경 유형 업데이트를 제출합니다. Amazon ECS 서비스에 대한 서비스 검색을 활성화하는 데 필요한 정보를 제공하려면 [서비스 검색 설명서를](#) 참조하세요.
- AMS는 현재 Amazon ECS Fargate의 컨테이너에 배포하는 데 사용되는 이미지를 관리하거나 제한하지 않습니다. Amazon ECR, Docker Hub 또는 기타 프라이빗 이미지 리포지토리에서 이미지를 배포할 수 있습니다. 따라서 퍼블릭 이미지 또는 보안되지 않은 이미지는 계정에 악의적인 활동이 발생할 수 있으므로 배포하지 않는 것이 좋습니다.

Q: AMS 계정에서 Fargate에서 Amazon ECS를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- 다음은 Fargate에서 Amazon ECS의 종속성입니다. 그러나 자체 프로비저닝된 역할로 이러한 서비스를 활성화하기 위한 추가 작업은 필요하지 않습니다.
 - CloudWatch 로그
 - CloudWatch 이벤트
 - CloudWatch 경보
 - CodeDeploy
 - App Mesh
 - 클라우드 맵

- Route 53
- 사용 사례에 따라 다음은 Amazon ECS가 의존하는 리소스이며 계정에서 Fargate에서 Amazon ECS를 사용하기 전에 필요할 수 있습니다.
 - Amazon ECS 서비스와 함께 사용할 보안 그룹입니다. 배포 | 고급 스택 구성 요소 | 보안 그룹 | 생성(자동)(ct-3pc215bnwb6p7)을 사용하거나, 보안 그룹에 특수 규칙이 필요한 경우 배포 | 고급 스택 구성 요소 | 보안 그룹 | 생성(검토 필요)(ct-1oxx2g2d7hc90)을 사용할 수 있습니다. 참고: Amazon ECS를 사용하여 선택한 보안 그룹은 Amazon ECS 서비스 또는 클러스터가 있는 Amazon ECS 전용으로 생성해야 합니다. 보안 그룹 섹션의 [Amazon ECS 설정](#) 및 [Amazon Elastic Container Service의 보안에서](#) 자세히 알아볼 수 있습니다.
 - 작업 간 로드 밸런싱을 위한 Application Load Balancer(ALB), Network Load Balancer(NLB), Classic Load Balancer(ELB).
 - ALBs.
 - Amazon ECS 클러스터와 통합할 앱 메시 리소스(예: 가상 라우터, 가상 서비스, 가상 노드).
- 현재 AMS가 표준 AMS 변경 유형 외부에서 생성될 때 지원 보안 그룹의 권한과 관련된 위험을 자동으로 완화할 수 있는 방법은 없습니다. Amazon ECS에서 사용하도록 지정되지 않은 보안 그룹을 사용할 가능성을 제한하려면 Fargate 클러스터와 함께 사용할 특정 보안 그룹을 요청하는 것이 좋습니다.

AMS SSP를 사용하여 AMS 계정 AWS Fargate 의에서 Amazon EKS 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Fargate Amazon EKS 기능에 액세스합니다. AWS Fargate 는 컨테이너에 대한 적절한 크기의 온디맨드 컴퓨팅 용량을 제공하는 기술입니다(컨테이너를 이해하려면 [컨테이너란 무엇입니까?](#) 참조). 를 사용하면 더 이상 컨테이너를 실행하기 위해 가상 머신 그룹을 프로비저닝, 구성 또는 확장할 필요가 AWS Fargate 없습니다. 따라서 서버 유형을 선택하거나, 노드 그룹을 조정할 시점을 결정하거나, 클러스터 패킹을 최적화할 필요가 없습니다.

Amazon Elastic Kubernetes Service(Amazon EKS)는 Kubernetes에서 제공하는 확장 가능한 업스트림 모델을 AWS Fargate 사용하여 구축된 컨트롤러를 AWS 사용하여 Kubernetes를와 통합합니다. 이러한 컨트롤러는 Amazon EKS 관리형 Kubernetes 컨트롤 플레인의 일부로 실행되며 Fargate에서 네이티브 Kubernetes 포드를 예약하는 역할을 합니다. Fargate 컨트롤러에는 여러 개의 변형 및 검증 승인 컨트롤러 외에도 기본 Kubernetes 스케줄러와 함께 실행되는 새 스케줄러가 포함되어 있습니다. Fargate에서 실행하기 위한 조건을 충족하는 포드를 시작하면 클러스터에서 실행되는 Fargate 컨트롤러가 해당 포드를 인식하고 업데이트하고 Fargate에 예약합니다.

자세한 내용은 Amazon [EKS on AWS Fargate Now Generally Available](#) 및 [Amazon EKS Best Practices Guide for Security](#)("Recommendations", "Review and revoke unnecessary anonymous access" 등 포함)를 참조하세요.

 Tip

AMS에는 Amazon EKS와 함께 사용할 수 있는 변경 유형인 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | OpenID Connect 공급자 생성(ct-30ecvfi3tq4k3)이 있습니다. 예제는 [Identity and Access Management\(IAM\) | OpenID Connect Provider 생성](#)을 참조하세요.

AWS Managed Services AWS Fargate 의 Amazon EKS FAQ

Q: AMS 계정에서 Fargate의 Amazon EKS에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다.

- customer_eks_fargate_console_role.

계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

- 이러한 서비스 역할은 Fargate의 Amazon EKS에 사용자를 대신하여 다른 AWS 서비스를 호출할 수 있는 권한을 부여합니다.

- customer_eks_pod_execution_role
- customer_eks_cluster_service_role

Q: AMS 계정에서 Fargate에서 Amazon EKS를 사용하는 데 따르는 제한 사항은 무엇인가요?

- [관리형](#) 또는 [자체 관리형](#) EC2 노드 그룹 생성은 AMS에서 지원되지 않습니다. EC2 작업자 노드를 사용해야 하는 경우 AMS Cloud Service Delivery Manager(CSDM) 또는 Cloud Architect(CA)에 문의하십시오.
- AMS에는 컨테이너 이미지에 대한 Trend Micro 또는 사전 구성된 네트워크 보안 구성 요소가 포함되지 않습니다. 배포 전에 자체 이미지 스캔 서비스를 관리하여 악성 컨테이너 이미지를 탐지해야 합니다.
- CloudFormation 상호 종속성으로 인해 EKSCTL이 지원되지 않습니다.

- 클러스터를 생성하는 동안 클러스터 컨트롤 플레인 로깅을 비활성화할 수 있는 권한이 있습니다. 자세한 내용을 알아보려면 [Amazon EKS 컨트롤 플레인 로깅](#)을 참조하세요. 클러스터 생성 시 모든 중요한 API, 인증 및 감사 로깅을 활성화하는 것이 좋습니다.
- 클러스터 생성 중에 Amazon EKS 클러스터에 대한 클러스터 엔드포인트 액세스는 기본적으로 퍼블릭으로 설정됩니다. 자세한 내용은 [Amazon EKS 클러스터 엔드포인트 액세스 제어](#)를 참조하세요. Amazon EKS 엔드포인트를 프라이빗으로 설정하는 것이 좋습니다. 퍼블릭 액세스에 엔드포인트가 필요한 경우 특정 CIDR 범위에 대해서만 엔드포인트를 퍼블릭으로 설정하는 것이 좋습니다.
- AMS에는 Amazon EKS Fargate의 컨테이너에 배포하는 데 사용되는 이미지를 강제로 적용하고 제한하는 방법이 없습니다. Amazon ECR, Docker Hub 또는 기타 프라이빗 이미지 리포지토리에서 이미지를 배포할 수 있습니다. 따라서 계정에서 악의적인 활동을 수행할 수 있는 퍼블릭 이미지를 배포할 위험이 있습니다.
- 클라우드 개발 키트(CDK) 또는 CloudFormation Ingest를 통한 EKS 클러스터 배포는 AMS에서 지원되지 않습니다.
- 수신 생성을 위해 매니페스트 파일에서 [ct-3pc215bnwb6p7 배포 | 고급 스택 구성 요소 | 보안 그룹 생성](#) 및 참조를 사용하여 필요한 보안 그룹을 생성해야 합니다. 이는 역할customer-eks-alb-ingress-controller-role이 보안 그룹을 생성할 권한이 없기 때문입니다.

Q: AMS 계정에서 Fargate에서 Amazon EKS를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

서비스를 사용하려면 다음 종속성을 구성해야 합니다.

- 서비스에 대해 인증하려면 KUBECTL과 aws-iam-authenticator를 모두 설치해야 합니다. 자세한 내용은 [클러스터 인증 관리](#)를 참조하세요.
- Kubernetes는 "서비스 계정"이라는 개념을 사용합니다. EKS의 kubernetes 클러스터 내에서 서비스 계정 기능을 활용하려면 다음 입력과 함께 관리 | 기타 | 기타 | RFC 업데이트가 필요합니다.
 - [필수] Amazon EKS 클러스터 이름
 - [필수] 서비스 계정(SA)이 배포될 Amazon EKS 클러스터 네임스페이스입니다.
 - [필수] Amazon EKS Cluster SA 이름입니다.
 - [필수] 연결할 IAM 정책 이름 및 권한/문서입니다.
 - [필수] 요청 중인 IAM 역할 이름입니다.
 - [선택 사항] OpenID Connect 공급자 URL입니다. 자세한 내용은 다음 단원을 참조하십시오.
 - [클러스터의 서비스 계정에 대한 IAM 역할 활성화](#)
 - [서비스 계정에 대한 세분화된 IAM 역할 소개](#)
- 에 대해 Config 규칙을 구성하고 모니터링하는 것이 좋습니다.

- 퍼블릭 클러스터 엔드포인트
- 비활성화된 API 로깅

이러한 Config 규칙을 모니터링하고 수정하는 것은 사용자의 책임입니다.

[ALB 수신 컨트롤러](#)를 배포하려면 관리 | 기타 | 기타 업데이트 RFC를 제출하여 ALB 수신 컨트롤러 포트와 함께 사용하는 데 필요한 IAM 역할을 프로비저닝합니다. ALB 수신 컨트롤러와 연결할 IAM 리소스를 생성하려면 다음 입력이 필요합니다(RFC에 포함).

- [필수] Amazon EKS 클러스터 이름
- [선택 사항] OpenID Connect 공급자 URL
- [선택 사항] 애플리케이션 로드 밸런서(ALB) 수신 컨트롤러 서비스가 배포될 Amazon EKS 클러스터 네임스페이스입니다. [기본값: kube-system]
- [선택 사항] Amazon EKS 클러스터 서비스 계정(SA) 이름. [기본값: aws-load-balancer-controller]

클러스터에서 봉투 보안 암호 암호화를 활성화하려면(권장) RFC의 설명 필드에 사용하려는 KMS 키 IDs를 제공하여 서비스를 추가합니다(관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가 (ct-1w8z66n899dct)). 봉투 암호화에 대한 자세한 내용은 [Amazon EKS에서 AWS KMS를 사용한 보안 암호에 대한 봉투 암호화 추가를 참조하세요](#).

AMS SSP를 사용하여 AMS 계정에서 Amazon EMR 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon EMR 기능에 직접 액세스할 수 있습니다. Amazon EMR은 Apache Spark, Apache Hive, Apache HBase, Apache Flink, Apache Hudi, Presto와 같은 오픈 소스 도구를 사용하여 방대한 양의 데이터를 처리하기 위한 업계 최고의 클라우드 빅 데이터 플랫폼입니다. Amazon EMR을 사용하면 기존 온프레미스 솔루션 비용의 절반 미만과 표준 Apache Spark보다 3배 빠른 속도로 페타바이트 규모의 분석을 실행할 수 있습니다. 단기 실행 작업의 경우 클러스터를 가동 및 가동 중지하고 사용된 인스턴스에 대해 초당 비용을 지불할 수 있습니다. 장기 실행 워크로드의 경우 수요에 맞게 자동으로 확장되는 고가용성 클러스터를 생성할 수 있습니다.

AMS 다중 계정 랜딩 존 또는 단일 계정 랜딩 존 계정에서 Amazon EMR 클러스터의 인스턴스를 하나 이상 생성하여 임시 및 영구 Amazon EMR 클러스터를 모두 지원할 수 있습니다. Kerberos 인증을 활성화하여 온프레미스 Active Directory 도메인에서 사용자를 인증할 수도 있습니다.

Amazon EMR 클러스터와 함께 여러 데이터 스토어를 활용하여 사용 사례별 하둡 도구 및 라이브러리를 지원할 수 있습니다. Amazon EMR 클러스터는 OnDemand 또는 스팟 인스턴스를 사용하여 생성하고 오토 스케일링을 구성하여 용량을 관리하고 비용을 절감할 수 있습니다.

클러스터 로그 파일은 로깅 및 디버깅을 위해 Amazon S3 버킷에 보관할 수 있습니다. Amazon EMR 클러스터에서 호스팅되는 웹 인터페이스에 액세스하여 hadoop 관리 요구 사항을 지원하거나 고객을 위한 노트북 경험을 지원할 수도 있습니다.

자세한 내용은 [Amazon EMR](#)을 참조하세요.

AWS Managed Services의 Amazon EMR FAQ

Q: AMS 계정에서 Amazon EMR에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다.

- customer_emr_cluster_instance_profile
- customer_emr_cluster_autoscaling_role
- customer_emr_console_role
- customer_emr_cluster_service_role

계정에 프로비저닝된 후에는 페더레이션 솔루션에서 customer_emr_console_role을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon EMR을 사용하는 데 따르는 제한 사항은 무엇인가요?

AWS 콘솔에서 EC2 클러스터에 Amazon EMR을 생성하는 동안 클러스터 생성 - 고급 옵션을 사용하는 것이 좋습니다. Amazon EMR 클러스터는 키가 "for-use-with-amazon-emr-managed-policies"이고 값이 "true"인 태그를 추가하여 생성해야 합니다. 보안 옵션에서 다음 구성을 선택합니다.

- 클러스터의 사용자 지정 역할을 선택합니다.
 - EMR 역할: customer_emr_cluster_service_role
 - EC2 인스턴스 프로파일: customer_emr_cluster_instance_profile
 - Auto Scaling 역할: customer_emr_cluster_autoscaling_role
- EC2 보안 그룹:
 - 마스터: ams-emr-master-security-group

- 코어 및 작업: `ams-emr-worker-security-group`
- 서비스 액세스: `ams-emr-serviceaccess-security-group`

Q: AMS 계정에서 Amazon EMR을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS는 Amazon EMR 마스터, 작업자 및 서비스 노드에 대한 기본 보안 그룹을 생성합니다.

Amazon EMR 클러스터와 함께 사용할 시작 템플릿 및 보안 그룹에는 "for-use-with-amazon-emr-managed-policies" 태그 키와 "true" 값이 있어야 합니다.

기본 Amazon EMR 클러스터 인스턴스 프로파일을 사용하면 이름이 "emr"을 포함하는 s3 버킷 및 dynamodb 테이블과 같은 리소스에 액세스할 수 있습니다. Amazon EMR에서 사용할 추가 리소스를 사용하도록 추가 IAM 정책을 요청할 수 있습니다. 다음 리소스 ARN은 `customer_emr_cluster_instance_profile`을 사용하여 Amazon EMR 작업에 사용할 수 있습니다.

- `arn:aws:dynamodb:*:*:table/*emr*`
- `arn:aws:kinesis:*:*:stream/*emr*`
- `arn:aws:sns:*:*:*emr*arn:aws:sqs:*:*:*emr*`
- `arn:aws:sqs:*:*:*emr*`
- `arn:aws:sqs:*:*:AWS-ElasticMapReduce-*`
- `arn:aws:sdb:*:*:domain:*emr*`
- `arn:aws:s3:::*emr*`

Amazon EMR 클러스터에 kerberos 인증이 필요한 경우:

- 각 각 각기 다른 Amazon EMR 클러스터에 사용할 영역 이름과 온프레미스 Active Directory IP 주소를 제공합니다.
- 인프라 요구 사항:

다중 계정 랜딩 존(MALZ): RFC를 제출하여 기존 애플리케이션 계정에서 새 관리형 애플리케이션 계정 또는 새 VPC를 생성합니다.

단일 계정 랜딩 존(SALZ): RFC를 제출하여 VPC에 새 서브넷을 생성합니다.

- 온프레미스 Active Directory에서 클러스터 영역에 대한 수신 신뢰를 구성합니다.
- 관리형 AD에서 영역에 대한 DNS 영역을 구성하려면 RFC를 제출합니다.

• 영역 구성:

MALZ: 관리 제출 | 기타 | 기타 | 업데이트(ct-0xdawir96cy7k) RFC를 업데이트하여 도메인 이름 접미사에 영역 이름을 사용하도록 VPC DHCP 옵션 세트를 업데이트합니다.

SALZ: 관리 제출 | 기타 | 기타 | 업데이트(ct-0xdawir96cy7k) RFC를 사용하여 도메인 이름 접미사에 특정 영역을 사용할 새 Amazon EMR AMI를 생성합니다.

Amazon EMR 스튜디오를 배포하려면 역할에 Amazon Simple Storage Service 버킷에 대한 사전 조건이 `customer_emr_cluster_service_role` 있습니다. 버킷을 생성하려면 자동 CTct-1a68ck03fn98r(배포 | 고급 스택 구성 요소 | S3 스토리지 | 생성)를 사용합니다. 이 자동 CT를 사용하여 Amazon EMR용 Amazon S3 버킷을 생성하는 경우 버킷 이름은 접두사로 시작해야 합니다. `customer-emr-*`. 또한 Amazon EMR 클러스터와 동일한 AWS 리전에 버킷을 생성해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon EventBridge 프로비저닝

AMS 자체 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon EventBridge 기능에 직접 액세스할 수 있습니다. Amazon EventBridge: 애플리케이션을 다양한 소스의 데이터와 쉽게 연결할 수 있는 서버리스 이벤트 버스 서비스입니다. EventBridge는 자체 애플리케이션, Software-as-a-Service(SaaS) 애플리케이션 및 AWS 서비스의 실시간 데이터 스트림을 제공하고 해당 데이터를와 같은 대상으로 라우팅합니다 AWS Lambda. 데이터를 전송할 대상을 결정하는 라우팅 규칙을 설정하여 모든 데이터 소스에 실시간으로 대응하는 애플리케이션 아키텍처를 구축할 수 있습니다. EventBridge를 사용하면 느슨하게 결합되고 분산되는 이벤트 기반 아키텍처를 구축할 수 있습니다.

자세한 내용은 [Amazon EventBridge](#)를 참조하세요.

AWS Managed Services FAQ의 EventBridge

Q: AMS 계정에서 EventBridge에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 EventBridge에 대한 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다 `customer_eventbridge_role` `customer_eventbridge_scheduler_execution_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

실행 역할은 EventBridge 스케줄러가 AWS 서비스 사용자를 대신하여 다른와 상호 작용하기 위해 수임하는 IAM 역할 `customer_eventbridge_scheduler_execution_role`입니다. 이 역할에 연결된 권한 정책은 EventBridge 스케줄러에 대상을 호출할 수 있는 액세스 권한을 부여합니다.

Note

기본적으로 EventBridge 스케줄러는 EventBridge에 AWS 소유 키를 사용하여 데이터를 암호화합니다. EventBridge의 고객 관리형 키를 사용하여 데이터를 암호화하려면 [관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 서비스 프로비저닝을 위한 변경 유형 추가\(검토 필요\)](#)(ct-3qe6io8t6jtny)를 사용하여 RFC를 제출합니다.

Q: AMS 계정에서 EventBridge를 사용하는 데 따르는 제한 사항은 무엇인가요?

AMS RFCs 제출하고 배치 작업을 트리거하는 서비스 역할, SQS 대기열, CodeBuild, CodePipeline 및 SSM 명령을 생성해야 합니다.

Q: AMS 계정에서 EventBridge를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

EventBridge를 사용하여 Lambda, Amazon SNS AWS Batch, Amazon SQS 또는 Amazon CloudWatch Logs AWS 리소스와 같은 다른 리소스를 트리거하기 전에 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 엔터티 또는 정책 생성(검토 필요) 변경 유형(ct-3dpd8mdd9jn1r)을 사용하여 RFC로 EventBridge 서비스 역할을 요청해야 합니다. 서비스 역할을 요청할 때 호출할 서비스를 지정합니다. 대상을 호출하는 데 필요한 권한에 대한 자세한 내용은 [EventBridge에 리소스 기반 정책 사용을 참조하세요](#).

EventBridge는 EventBridge AWS 서비스에서 사용자 AWS CloudTrail, 역할 또는가 수행한 작업에 대한 레코드를 제공하는 서비스와 통합됩니다. CloudTrail을 활성화하고 로그 파일을 S3 버킷에 저장할 수 있어야 합니다. 참고: 모든 AMS 계정에는 CloudTrail이 활성화되어 있으므로 별도의 조치가 필요하지 않습니다.

Q: customer_eventbridge_scheduler_execution_role 역할에는 AWS Key Management Service 키에 대한 사전 조건이 있습니다(암호화에 사용되는 경우 선택 사항). 저장/전송 시 데이터 암호화에 AWS KMS CMKs 채택하려면 어떻게 해야 하나요?

기본적으로 EventBridge 스케줄러는 AWS 소유 키(저장 시 암호화)에 저장된 이벤트 메타데이터 및 메시지 데이터를 암호화합니다. 또한 EventBridge 스케줄러는 전송 계층 보안(TLS)(전송 중 암호화)을 사용하여 EventBridge 스케줄러와 다른 서비스 간에 전달하는 데이터를 암호화합니다.

특정 사용 사례에서 EventBridge 스케줄러에서 데이터를 보호하는 암호화 키를 제어하고 감사해야 하는 경우 고객 관리형 키를 사용할 수 있습니다.

Amazon EventBridge를 사용하여 AWS KMS 권한을 온보딩하기 전에 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(검토 필요)를 사용하여 RFC를 요청해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Forecast 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Forecast(Forecast) 기능에 직접 액세스할 수 있습니다. Amazon Forecast는 기계 학습을 사용하여 매우 정확한 예측을 제공하는 완전관리형 서비스입니다.

Note

AWS 는 2024년 7월 29일부터 Amazon Forecast에 대한 신규 고객 액세스를 종료했습니다. Amazon Forecast 기존 고객은 평소와 같이 서비스를 계속 사용할 수 있습니다. Amazon Forecast의 보안, 가용성 및 성능 개선에 AWS 계속 투자하지만 새로운 기능을 도입할 계획 AWS 은 없습니다.

Amazon Forecast를 사용하려면 CSDM에 문의하여 Amazon [Forecast 사용량을 Amazon SageMaker Canvas로 전환하는](#) 방법에 대해 자세히 알아보세요.

Forecast는 Amazon.com 사용된 것과 동일한 기술을 기반으로 기계 학습을 사용하여 시계열 데이터를 추가 변수와 결합하여 예측을 구축합니다. Forecast를 시작하려면 기계 학습 경험이 필요하지 않습니다. 과거 데이터와 예측에 영향을 미칠 수 있다고 생각되는 추가 데이터만 제공하면 됩니다. 예를 들어, 셔츠의 특정 색상에 대한 수요는 계절과 매장 위치에 따라 변경될 수 있습니다. 이 복잡한 관계는 자체적으로 결정하기 어렵지만 기계 학습은 이를 인식하는 데 이상적입니다. 데이터를 제공하면 Forecast는 시계열 데이터만 보는 것보다 최대 50% 더 정확한 예측을 수행할 수 있는 예측 모델을 자동으로 검사하고 의미 있는 것을 식별하며 생성합니다.

자세한 내용은 [Amazon Forecast](#)를 참조하세요.

AWS Managed Services FAQ의 Amazon Forecast

Q: AMS 계정에서 Forecast에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 AWS Firewall Manager 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_forecast_admin_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Forecast를 사용하는 데 따르는 제한 사항은 무엇인가요?

기본 S3 버킷 액세스는 이름 지정 패턴이 'customer-forecast-*'인 버킷에만 액세스할 수 있도록 허용합니다. 데이터 버킷에 대한 고유한 이름 지정 규칙이 있는 경우 Cloud Architect(CA)와 버킷 이름 지정 및 관련 액세스 설정에 대해 논의합니다. 예:

- 'AmazonForecast-ExecutionRole-*' 및 관련 적절한 S3 버킷 액세스와 같은 이름을 지정하여 특정 Amazon Forecast 서비스 역할을 정의할 수 있습니다. ExecutionRole S3 IAM 콘솔에서 서비스 역할 - AmazonForecast-ExecutionRole-Admin 및 IAM 정책 - customer_forecast_default_s3_access_policy를 참조하세요.
- 관련 S3 버킷 액세스를 IAM 페더레이션 역할에 연결해야 할 수 있습니다. IAM 콘솔에서 IAM 정책 - customer_forecast_default_s3_access_policy를 참조하세요.

Q: AMS 계정에서 Forecast를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- Forecast를 사용하기 전에 적절한 Amazon S3 버킷(들)을 생성해야 합니다. 특히 기본 S3 버킷 액세스는 'customer-forecast-*'라는 이름 지정 패턴을 사용합니다.
- 'customer-forecast-*' 이외의 S3 버킷에서 이름 지정 패턴을 사용하려면 버킷에 대한 S3 액세스 권한이 있는 새 서비스 역할을 생성해야 합니다.
 1. 'AmazonForecast-ExecutionRole-{suffix}'라는 이름으로 생성할 새 서비스 역할입니다.
 2. customer_forecast_default_s3_access_policy와 유사하고 새 서비스 역할 및 관련 페더레이션 관리자 역할(예: 'customer_forecast_admin_role')과 연결되는 새 IAM 정책 생성

Q: Amazon Forecast를 사용하는 동안 데이터 보안을 강화하려면 어떻게 해야 하나요?

- 저장 데이터 암호화의 경우 AWS KMS를 사용하여 고객 관리형 CMK를 프로비저닝하여 Amazon S3 서비스의 데이터 스토리지를 보호할 수 있습니다.
 - 프로비저닝 키를 사용하여 버킷에서 기본 암호화를 활성화하고 데이터를 입력하는 동안 AWS KMS 데이터 암호화를 수락하도록 버킷 정책을 설정합니다.
 - Amazon Forecast 서비스 역할 'AmazonForecast-ExecutionRole-*' 및 페더레이션 관리자 역할(예: 'customer_forecast_admin_role')을 AWS KMS 키 사용자로 활성화합니다.
- 전송 중 데이터 암호화의 경우 Amazon S3 버킷 정책에서 객체를 전송하는 데 필요한 HTTPS 프로토콜을 설정할 수 있습니다.
- 액세스 제어에 대한 추가 제한에서 Amazon Forecast 서비스 역할 'AmazonForecast-ExecutionRole-*' 및 관리자 역할(예: 'customer_forecast_admin_role')에 대해 승인된 액세스에 대한 버킷 정책을 활성화합니다.

Q: Amazon Forecast 사용 시 모범 사례는 무엇인가요?

- Amazon Forecast에서 S3 버킷을 사용하는 동안 데이터 분류 관행을 잘 이해하고 관련 데이터 보안 요구 사항을 매핑해야 합니다.
- Amazon S3 버킷 구성의 경우 S3 버킷 정책에서 HTTPS 적용을 활성화하는 것이 좋습니다.
- 'customer-forecast-*'라는 이름의 Amazon S3 버킷에 대한 관리자 역할 'customer_forecast_admin_role' 지원 허용 액세스(Get/Delete/Put S3 객체)를 알고 있어야 합니다.
참고: 여러 팀에 대한 세분화된 액세스 제어가 필요한 경우 다음 관행을 따르세요.
- 관련 Amazon S3 버킷에 대한 최소 권한 액세스를 사용하여 팀 기반 액세스 IAM 자격 증명(역할/사용자)을 정의합니다.
- 팀/프로젝트 기반 AWS KMS CMKs 생성하면 해당 IAM 자격 증명에 대한 적절한 액세스 권한이 부여됩니다(사용자 액세스 및 'AmazonForecast-ExecutionRole-{team/project}').
- 생성된 AWS KMS CMKs를 사용하여 S3 버킷 기본 암호화를 설정합니다.
- S3 버킷 정책에 HTTPS 프로토콜을 사용하여 S3 API 트래픽을 적용합니다.
- 관련 IAM 자격 증명(사용자 액세스 및 'AmazonForecast-ExecutionRole-{team/project}')에 대한 승인된 액세스에 대해 S3 버킷 구성을 버킷에 적용합니다.
- 'customer_forecast_admin_role'을 범용으로 사용하려면 이전에 나열된 포인트를 고려하여 S3 버킷을 보호하세요.

Q: Amazon Forecast에 대한 규정 준수 정보는 어디에 있나요?

[AWS 서비스 규정 준수 프로그램을](#) 참조하세요.

AMS SSP를 사용하여 AMS 계정에서 Amazon FSx 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon FSx 기능에 직접 액세스할 수 있습니다. Amazon FSx는 완전 관리형 타사 파일 시스템을 제공합니다. Amazon FSx는 Windows 기반 스토리지, 고성능 컴퓨팅(HPC), 기계 학습, 전자 설계 자동화(EDA)와 같은 워크로드를 위한 기능 세트와 타사 파일 시스템의 기본 호환성을 제공합니다. Amazon FSx는 하드웨어 프로비저닝, 소프트웨어 구성, 패치 적용 및 백업과 같이 시간이 많이 걸리는 관리 작업을 자동화합니다. Amazon FSx는 파일 시스템을 클라우드 네이티브 AWS 서비스와 통합하여 더 광범위한 워크로드 세트에 훨씬 더 유용합니다.

Amazon FSx는 Windows 기반 애플리케이션용 Amazon FSx for Windows File Server와 컴퓨팅 집약적인 워크로드용 Amazon FSx for Lustre라는 두 가지 파일 시스템 중에서 선택할 수 있습니다. 자세한 내용은 [Amazon FSx](#)를 참조하세요.

AWS Managed Services의 Amazon FSx FAQ

Q: AMS 계정에서 Amazon FSx에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon FSx에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다: `customer_fsx_admin_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon FSx를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. 서비스의 전체 기능을 사용할 수 있습니다.

Q: AMS 계정에서 Amazon FSx를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

사전 조건은 없습니다. 그러나 다중 AZ와 같은 고급 구성의 경우 DFS 복제 및 DFS 네임스페이스 서비스를 설치하고 관리해야 합니다. 자세한 내용은 [다중 AZ 파일 시스템 배포를 참조하세요](#).

Q: Amazon FSx 파일 시스템을 다중 계정 랜딩 존 Managed AD와 통합하려면 어떻게 해야 하나요?

Amazon FSx 파일 시스템을 생성할 때 MALZ Managed AD를 Windows 인증을 위한 'AWS 관리형 Microsoft Active Directory'로 지정할 수 있습니다. 자세한 내용은 [Microsoft Active Directory AWS Directory Service 용에서 Amazon FSx 사용을 참조하세요](#).

또한 먼저 Managed AD를 애플리케이션 계정과 공유해야 합니다. 관리 | 디렉터리 서비스 | 디렉터리 | 디렉터리 변경 유형 공유(ct-369odosk0pd9w)를 사용하여 RFC를 제출하여 이 작업을 수행합니다.

Q: AWS 위임 FSx 관리자 그룹에 속한 사용자는 누구입니까?

IT 파일 서버 관리자만. 이 그룹에는 모든 파일 공유에 대한 전체 액세스 권한이 있습니다.

Q: FSx 시스템이 프로비저닝될 때 생성되는 기본 파일 공유, 공유를 사용해야 합니까?

아니요. 프로비저닝된 대로 기본 파일 공유, 공유를 사용하지 않는 것이 좋습니다. 최소 권한 원칙을 위반하는 모든 사람에게 전체 액세스 권한을 부여합니다. 대신 비즈니스 요구 사항에 맞는 더 작은 사용자 지정 파일 공유를 생성합니다.

Q: 내 비즈니스의 특정 조직에 대한 사용자 지정 파일 공유를 생성하려면 어떻게 해야 하나요?

사용자 지정 [파일 공유 생성에 대한 지침은 파일 공유](#)를 참조하세요. 최소 권한 원칙을 사용하여 각 파일 공유에 대한 액세스를 제한합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon FSx for OpenZFS 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon FSx for OpenZFS 기능에 직접 액세스할 수 있습니다. FSx for OpenZFS는 애플리케이션 코드 또는 데이터 관리 방법을 변경하지 않고도 온프레미스 ZFS 또는 기타 Linux 기반 파일 서버에 있는 데이터를 AWS로 쉽게 이동할 수 있는 완전 관리형 파일 스토리지 서비스입니다. 오픈 소스 OpenZFS 파일 시스템에 구축된 매우 안정적이고 확장 가능하며 성능이 뛰어나고 기능이 풍부한 파일 스토리지를 제공하여 OpenZFS 파일 시스템의 친숙한 기능과 기능에 완전 관리형 AWS 서비스의 민첩성, 확장성 및 단순성을 제공합니다. 클라우드 네이티브 애플리케이션을 구축하는 개발자를 위해 데이터 작업을 위한 풍부한 기능을 갖춘 간단한 고성능 스토리지를 제공합니다.

FSx for OpenZFS 파일 시스템은 업계 표준 NFS 프로토콜(v3, v4.0, v4.1, v4.2)을 사용하여 Linux, Windows 및 macOS 컴퓨팅 인스턴스 및 컨테이너에서 광범위하게 액세스할 수 있습니다. AWS Graviton 프로세서와 최신 AWS 디스크 및 네트워킹 기술(AWS Scalable Reliable Datagram 네트워킹 및 AWS Nitro 시스템 포함)로 구동되는 FSx for OpenZFS는 수백 마이크로초의 지연 시간으로 최대 100만 IOPS를 제공합니다. 즉각적인 point-in-time 스냅샷 및 데이터 복제와 같은 OpenZFS 기능을 완벽하게 지원하는 FSx for OpenZFS를 사용하면 온프레미스 파일 서버를 익숙한 파일 시스템 기능을 제공하고 긴 검증을 수행하고 기존 애플리케이션 또는 도구를 변경하거나 재설계할 필요가 없는 AWS 스토리지로 쉽게 교체할 수 있습니다. 또한 OpenZFS 데이터 관리 기능의 성능과 최신 AWS 기술의 고성능 및 비용 효율성을 결합하여 FSx for OpenZFS를 사용하면 고성능의 데이터 집약적인 애플리케이션을 구축하고 실행할 수 있습니다.

완전 관리형 서비스인 FSx for OpenZFS를 사용하면에서 완전 관리형 파일 시스템을 쉽게 시작, 실행 및 확장하여 온프레미스에서 실행하는 파일 서버를 AWS 대체하는 동시에 민첩성을 높이고 비용을 절감할 수 있습니다. FSx for OpenZFS를 사용하면 파일 서버 및 스토리지 볼륨 설정 및 프로비저닝, 데이터 복제, 파일 서버 소프트웨어 설치 및 패치, 하드웨어 장애 감지 및 해결, 백업 수동 수행에 대해 더 이상 걱정할 필요가 없습니다. 또한 AWS Identity and Access Management (IAM), AWS Key Management Service (), Amazon CloudWatch 및 같은 다른 AWS 서비스와의 풍부한 통합 AWS KMS를 제공합니다 AWS CloudTrail.

Amazon FSx는 Windows 기반 애플리케이션용 Amazon FSx for Windows File Server와 컴퓨팅 집약적인 워크로드용 Amazon FSx for Lustre라는 두 가지 파일 시스템 중에서 선택할 수 있습니다. 자세한 내용은 [Amazon FSx](#)를 참조하세요.

AWS Managed Services FAQ의 Amazon FSx for OpenZFS

Q: AMS 계정에서 FSx for OpenZFS를 사용하기 위해 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon FSx OpenZFS에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_fsx_ontap_admin_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정에서 FSx for OpenZFS를 사용할 때 적용되는 제한 사항은 무엇인가요?

Amazon FSx 탄력적 네트워크 인터페이스(ENIs)의 보안 그룹을 교체하려면 보안 그룹이 AMS 환경의 중요한 경계이므로 관리 | 기타 | 기타 | RFCs 업데이트를 제출해야 합니다. 이것이 유일한 제한입니다.

Q: AMS 계정에서 FSx for OpenZFS를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

사전 조건은 없습니다. 그러나 [AMS SSP를 사용하여 AMS 계정에서 Amazon FSx 프로비저닝](#) 설치되어 있어야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon FSx for NetApp ONTAP 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon FSx for NetApp ONTAP 기능에 직접 액세스할 수 있습니다. Amazon FSx for NetApp ONTAP은 NetApp의 인기 있는 ONTAP 파일 시스템을 기반으로 구축된 매우 안정적이고 확장 가능하며 성능이 뛰어나고 기능이 풍부한 파일 스토리지를 제공하는 완전관리형 서비스입니다. NetApp 파일 시스템의 친숙한 기능, 성능, 기능 및 APIs에 완전 관리형의 민첩성, 확장성 및 단순성을 제공합니다 AWS 서비스.

Amazon FSx for NetApp ONTAP은 AWS 또는 온프레미스에서 실행되는 Linux, Windows 및 macOS 컴퓨팅 인스턴스에서 광범위하게 액세스할 수 있는 기능이 풍부하고 빠르고 유연한 공유 파일 스토리지를 제공합니다. FSx for ONTAP은 밀리초 미만의 지연 시간으로 고성능 SSD 스토리지를 제공하며 버튼 클릭만으로 파일을 스냅샷 처리, 복제 및 복제할 수 있으므로 데이터를 빠르고 쉽게 관리할 수 있습니다. 또한 데이터를 저비용의 탄력적 스토리지로 자동 계층화하므로 용량을 프로비저닝하거나 관리할 필요가 없으며 소량의 데이터에 대해서만 SSD 스토리지 비용을 지불하면서 워크로드에 대해 SSD 수준의 성능을 달성할 수 있습니다. 완전 관리형 백업과 교차 리전 재해 복구 지원을 통해 가용성과 내구성이 뛰어난 스토리지를 제공하고 널리 사용되는 데이터 보안 및 바이러스 백신 애플리케이션을 지원하여 데이터를 더 쉽게 보호하고 보호할 수 있습니다. 온프레미스에서 NetApp ONTAP을 사용하는 고객의 경우 FSx for ONTAP은 애플리케이션 코드 또는 데이터 관리 방법을 변경할 필요 없이 파일 기반 애플리케이션을 온프레미스에서 로 마이그레이션, 백업 또는 버스트하는 데 이상적인 솔루션입니다.

완전 관리형 서비스인 Amazon FSx for NetApp ONTAP을 사용하면 클라우드에서 안정적이고 성능이 뛰어나며 안전한 공유 파일 스토리지를 간단하게 시작하고 확장할 수 있습니다. Amazon FSx for

NetApp ONTAP을 사용하면 파일 서버 및 스토리지 볼륨 설정 및 프로비저닝, 데이터 복제, 파일 서버 소프트웨어 설치 및 패치, 하드웨어 장애 감지 및 해결, 장애 조치 및 장애 복구 관리, 백업 수동 수행에 대해 더 이상 걱정할 필요가 없습니다. 또한 AWS Identity and Access Management Amazon WorkSpaces AWS Key Management Service 및와 AWS 서비스같은 다른와 풍부한 통합을 제공합니다 AWS CloudTrail.

Amazon FSx는 Windows 기반 애플리케이션용 Amazon FSx for Windows File Server와 컴퓨팅 집약적인 워크로드용 Amazon FSx for Lustre라는 두 가지 파일 시스템 중에서 선택할 수 있습니다. 자세한 내용은 [Amazon FSx](#)를 참조하세요.

AWS Managed Services FAQ의 Amazon FSx for NetApp ONTAP

Q: AMS 계정에서 Amazon FSx for NetApp ONTAP에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon FSx for NetApp ONTAP에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_fsx_ontap_admin_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon FSx for NetApp ONTAP 사용에 대한 제한 사항은 무엇입니까?

Amazon FSx for NetApp ONTAP 탄력적 네트워크 인터페이스(ENIs)의 보안 그룹을 교체하려면 보안 그룹이 AMS 환경의 중요한 경계이므로 관리 | 기타 | 기타 | RFCs 업데이트를 제출해야 합니다. 이것이 유일한 제한입니다.

Q: AMS 계정에서 Amazon FSx for NetApp ONTAP을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

사전 조건은 없습니다. 그러나 [AMS SSP를 사용하여 AMS 계정에서 Amazon FSx 프로비저닝](#) 설치되어 있어야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Inspector Classic 프로비저닝

Note

지원 종료 공지: 2026년 5월 20일에 Amazon Inspector Classic에 대한 지원이 AWS 종료됩니다. 2026년 5월 20일 이후에는 Amazon Inspector Classic 콘솔 또는 Amazon Inspector Classic 리소스에 더 이상 액세스할 수 없습니다. Amazon Inspector Classic은 더 이상 새 계정과 지난 6개월 동안 평가를 완료하지 않은 계정에서 사용할 수 없습니다. 다른 모든 계정의 경우 액세스는 2026년 5월 20일까지 유효하며, 그 이후에는 Amazon Inspector Classic 콘솔 또는 Amazon

Inspector Classic 리소스에 더 이상 액세스할 수 없습니다. 자세한 내용은 [Amazon Inspector Classic 지원 종료를 참조하세요](#).

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Inspector Classic 기능에 직접 액세스할 수 있습니다. Amazon Inspector Classic은 배포된 애플리케이션의 보안 및 규정 준수를 개선하는 데 도움이 되는 자동화된 보안 평가 서비스입니다. AWS. Amazon Inspector Classic은 애플리케이션의 노출, 취약성 및 모범 사례와의 편차를 자동으로 평가합니다. 평가를 수행한 후 Amazon Inspector Classic은 심각도 수준에 따라 우선순위가 지정된 보안 조사 결과의 세부 목록을 생성합니다. 이러한 결과는 직접 검토하거나 Amazon Inspector Classic 콘솔 또는 API를 통해 사용할 수 있는 세부 평가 보고서의 일부로 검토할 수 있습니다. 자세한 내용은 [Amazon Inspector Classic](#)을 참조하세요.

AWS Managed Services FAQ의 Amazon Inspector

Q: AMS 계정에서 Amazon Inspector Classic에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon Inspector Classic에 대한 액세스를 요청합니다. 이 RFC는 계정에 `customer_inspector_admin_role` IAM 역할을 프로비저닝합니다. 역할에는 AWS관리형 `AmazonInspectorFullAccess` 정책이 포함됩니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Inspector Classic을 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Inspector Classic의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Inspector Classic을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon Inspector Classic을 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS에서 새 Amazon Inspector 사용

이제 AMS 계정에서 새 Amazon Inspector를 사용할 수 있습니다.

Amazon Inspector Classic의 경우 `customer-inspector-admin-role-ssm-inspector-agent-policy` 및 `customer-inspector-admin-role`이제 추가를 포함하는 SSPS 역할가 업데이트되었습니다. `customer-inspector-admin-role`이제 `AmazonInspector2FullAccess` 정책을 포함합니다. 이 새 정책은 새 버전의 Amazon Inspector에 대한 API 권한을 허용합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Kendra 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Kendra 기능에 직접 액세스할 수 있습니다. Amazon Kendra는 자연어 처리 및 고급 기계 학습 알고리즘을 사용하여 데이터의 검색 질문에 대한 특정 답변을 반환하는 지능형 검색 서비스입니다. 기존 키워드 기반 검색과 달리 Amazon Kendra는 시맨틱 및 컨텍스트 이해 기능을 사용하여 문서가 검색 쿼리와 관련이 있는지 확인합니다. Amazon Kendra는 질문에 대한 구체적인 답변을 반환하므로 경험이 인간 전문가와의 상호 작용에 가깝습니다. Amazon Kendra는 확장성이 뛰어나고 성능 요구 사항을 충족할 수 있으며 Amazon S3 및 Amazon Lex와 같은 다른 AWS 서비스와 긴밀하게 통합되고 엔터프라이즈급 보안을 제공합니다. 자세한 내용은 [Amazon Kendra](#)를 참조하세요.

AWS Managed Services FAQ의 Amazon Kendra

Q: AMS 계정에서 Amazon Kendra에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Amazon Inspector Classic에 대한 액세스를 요청하려면 Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출합니다. 이 RFC는 계정에 customer_kendra_console_role IAM 역할을 프로비저닝합니다. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Kendra를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Kendra의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Kendra를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon Kendra를 시작하기 위한 사전 조건이나 종속성은 없습니다. 그러나 특정 사용 사례에 따라 다른 AWS 서비스에 대한 액세스가 필요할 수 있습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Kinesis Data Streams 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Kinesis Data Streams(KDS) 기능에 직접 액세스할 수 있습니다. Amazon Kinesis Data Streams는 확장성과 내구성이 뛰어난 실시간 데이터 스트리밍 서비스입니다. KDS는 웹 사이트 클릭스트림, 데이터베이스 이벤트 스트림, 금융 거래, 소셜 미디어 피드, IT 로그, 위치 추적 이벤트와 같은 수십만 개의 소스에서 초당 기가바이트의 데이터를 지속적으로 캡처할 수 있습니다. 수집된 데이터는 밀리초 단위로 실시간 대시보드, 실시간 이상 탐지, 동적 요금 등과 같은 실시간 분석 사용 사례를 가능하게 합니다. 자세한 내용은 [Amazon Kinesis Data Streams](#)를 참조하세요.

AWS Managed Services FAQ의 Kinesis Data Streams

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Kinesis Data Streams에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 Amazon Kinesis Data Streams에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 `customer_kinesis_data_streaming_user_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Kinesis Data Streams를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Kinesis Data Streams의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Kinesis Data Streams를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon Kinesis Data Streams를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Kinesis Video Streams 프로비저닝

AMS 자체 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Amazon Kinesis Video Streams(KVS) 기능에 액세스할 수 있습니다. Amazon Kinesis Video Streams를 사용하면 분석, 기계 학습(ML), 재생 및 기타 처리를 AWS 위해 연결된 디바이스에서 로 비디오를 안전하게 스트리밍할 수 있습니다. Kinesis Video Streams는 수백만 개의 디바이스에서 스트리밍 비디오 데이터를 수집하는 데 필요한 모든 인프라를 자동으로 프로비저닝하고 탄력적으로 확장합니다. 또한 스트림에 비디오 데이터를 안정적으로 저장, 암호화 및 인덱싱하고 easy-to-use APIs를 통해 데이터에 액세스할 수 있습니다. Kinesis Video Streams를 사용하면 라이브 및 온디맨드 보기를 위해 비디오를 재생하고 Amazon Rekognition Video와의 통합을 통해 컴퓨터 비전 및 비디오 분석을 활용하는 애플리케이션과 Apache MxNet, TensorFlow, OpenCV와 같은 ML 프레임워크용 라이브러리를 빠르게 구축할 수 있습니다. 자세한 내용은 [Amazon Kinesis Video Streams](#) 참조하세요.

AWS Managed Services FAQ의 Amazon Kinesis Video Streams

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Kinesis Video Streams해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 Amazon Kinesis Video Streams에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_kinesis_video_streaming_user_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Kinesis Video Streams를 사용할 때 적용되는 제한 사항은 무엇인가요?

제한은 없습니다. Amazon Kinesis Video Streams의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Kinesis Video Streams를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon Kinesis Video Streams를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Lex 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Lex 기능에 직접 액세스할 수 있습니다. Amazon Lex는 음성과 텍스트를 사용하여 모든 애플리케이션에 대화형 인터페이스를 구축하는 서비스입니다. Amazon Lex는 음성을 텍스트로 변환하기 위한 자동 음성 인식(ASR)과 텍스트의 의도를 인식하기 위한 자연어 이해(NLU)의 고급 딥 러닝 기능을 제공하여 매우 매력적인 사용자 경험과 생생한 대화형 상호 작용으로 애플리케이션을 구축할 수 있습니다. Amazon Lex를 사용하면 이제 모든 개발자가 Amazon Alexa를 지원하는 것과 동일한 딥 러닝 기술을 사용할 수 있으므로 정교한 자연어, 대화형 봇 또는 챗봇을 빠르고 쉽게 구축할 수 있습니다. 자세한 내용은 [Amazon Lex](#)를 참조하세요.

AWS Managed Services의 Amazon Lex FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Lex에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_lex_author_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Lex를 사용할 때 제한 사항은 무엇인가요?

Amazon Lex와 Lambda의 통합은 AMS 인프라의 수정을 방지하기 위해 "AMS-" 접두사가 없는 Lambda 함수로 제한됩니다.

Q: AMS 계정에서 Amazon Lex를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon Lex를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon MQ 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon MQ 기능에 직접 액세스할 수 있습니다. Amazon MQ는 클라우드에서 메시지 브로커를 설정하고 운영하는 데 도움이 되는 Apache ActiveMQ용 관리형 메시지 브로커 서비스입니다. 메시지 브로커를 사용하면 서로 다른 소프트웨어 시스템이 서로 다른 프로그래밍 언어를 사용하고 플랫폼에서 정보를 통신하고 교환할 수 있습니다. Amazon MQ는 인기 있는 오픈 소스 메시지 브로커인 ActiveMQ의 프로비저닝, 설정 및 유지 관리를 관리하여 운영 부하를 줄입니다. 현재 애플리케이션을 Amazon MQ에 연결하면 JMS, NMS, AMQP, STOMP, MQTT 및 WebSocket을 포함한 메시징에 업계 표준 APIs 및 프로토콜이 사용됩니다. 표준을 사용하면 대부분의 경우로 마이그레이션할 때 메시징 코드를 다시 작성할 필요가 없습니다. AWS. 자세한 내용은 [Amazon MQ란 무엇입니까?](#)를 참조하세요.

AWS Managed Services의 Amazon MQ FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon MQ에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AMS 계정에서 Amazon MQ를 사용하는 과정은 2단계로 이루어집니다.

1. Amazon MQ 브로커를 프로비저닝합니다. 이렇게 하려면 Amazon MQ 브로커가 포함된 CFN 템플릿을 배포 | 수집 | CloudFormation 템플릿의 스택 | 변경 유형 생성(ct-36cn2avfrj9v)이 있는 RFC를 통해 제출하거나, 관리 | 기타 | 기타 | 변경 유형 생성(ct-1e1xtak34nx76)이 있는 RFC를 제출하여 Amazon MQ 브로커가 계정에 프로비저닝되도록 요청합니다.
2. Amazon MQ 콘솔에 액세스합니다. Amazon MQ 브로커가 프로비저닝된 후 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 Amazon MQ 콘솔에 액세스할 수 있습니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_mq_console_role.

계정에 역할이 프로비저닝된 후 페더레이션 솔루션에 온보딩해야 합니다.

Q: AMS 계정에서 Amazon MQ를 사용하는 데 따르는 제한 사항은 무엇인가요?

Amazon MQ의 전체 기능은 AMS 계정에서 사용할 수 있지만, 필요한 승격된 권한으로 인해 정책을 통해 Amazon MQ 브로커를 프로비저닝할 수 없습니다. 계정에서 Amazon MQ 브로커를 프로비저닝하는 방법에 대한 자세한 내용은 위의 섹션을 참조하세요.

Q: AMS 계정에서 Amazon MQ를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 Amazon MQ를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Managed Service for Apache Flink 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Amazon Managed Service for Apache Flink 기능에 액세스할 수 있습니다. Managed Service for Apache Flink는 스트리밍 데이터를 분석하고, 실행 가능한 인사이트를 얻고, 비즈니스 및 고객 요구 사항에 실시간으로 대응하는 가장 쉬운 방법입니다. Amazon Managed Service for Apache Flink는 스트리밍 애플리케이션을 빌드, 관리 및 다른 AWS 서비스와 통합하는 복잡성을 줄여줍니다. SQL 사용자는 템플릿과 대화형 SQL 편집기를 사용하여 스트리밍 데이터를 쉽게 쿼리하거나 전체 스트리밍 애플리케이션을 빌드할 수 있습니다. Java 개발자는 오픈 소스 Java 라이브러리 및 AWS 통합을 사용하여 정교한 스트리밍 애플리케이션을 빠르게 구축하여 데이터를 실시간으로 변환하고 분석할 수 있습니다. Amazon Managed Service for Apache Flink는 실시간 애플리케이션을 지속적으로 실행하는 데 필요한 모든 것을 처리하며 수신 데이터의 볼륨과 처리량에 맞게 자동으로 확장됩니다. Amazon Managed Service for Apache Flink를 사용하면 스트리밍 애플리케이션이 사용하는 리소스에 대해서만 비용을 지불하면 됩니다. 최소 요금이나 설정 비용은 없습니다. 자세한 내용은 [Amazon Managed Service for Apache Flink](#)를 참조하세요.

AWS Managed Services FAQ의 Managed Service for Apache Flink

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Managed Service for Apache Flink에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_kinesis_analytics_application_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Managed Service for Apache Flink를 사용하는 데 따르는 제한 사항은 무엇인가요?

- 구성은 AMS 인프라 수정을 방지하기 위해 'AMS-' 또는 'MC-' 접두사가 없는 리소스로 제한됩니다.
- 새 Kinesis Data Streams 또는 Firehose를 삭제하거나 생성할 수 있는 권한이 정책에서 제거되었습니다. 이를 허용하는 또 다른 정책이 있습니다.

Q: AMS 계정에서 Amazon Kinesis Data Streams를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

몇 가지 종속성이 있습니다.

- Amazon Managed Service for Apache Flink를 사용하려면 Managed Service for Apache Flink로 애플리케이션을 구성하기 전에 Kinesis Data Streams 또는 Firehose를 생성해야 합니다.
- 리소스 기반 정책 권한은 특정 입력 데이터 소스를 나타내야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Managed Streaming for Apache Kafka 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Amazon Managed Streaming for Apache Kafka(Amazon MSK) 기능에 액세스할 수 있습니다. Amazon Managed Streaming for Apache Kafka는 완전 관리형 AWS 스트리밍 데이터 서비스이므로 Apache Kafka 클러스터 운영 전문가가 될 필요 없이 Apache Kafka를 사용하여 스트리밍 데이터를 처리하는 애플리케이션을 쉽게 구축하고 실행할 수 있습니다. Amazon MSK는 Apache Kafka 클러스터 및 Apache ZooKeeper 노드의 프로비저닝, 구성 및 유지 관리를 관리합니다. Amazon MSK는 AWS 콘솔에 주요 Apache Kafka 성능 지표도 표시합니다.

Amazon MSK는 VPC 네트워크 격리, 컨트롤 플레인 API 권한 부여를 위한 AWS IAM, 유틸리티 암호화, 전송 중 TLS 암호화, TLS 기반 인증서 인증,에서 보호되는 SASL/SCRAM 인증 등 Apache Kafka 클러스터에 대한 여러 수준의 보안을 제공합니다 AWS Secrets Manager. 자세한 내용은 [Amazon MSK](#)를 참조하세요.

AWS Managed Services의 Amazon MSK FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon MSK에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 정책 및 역할을 프로비저닝합니다.

- customer-msk-admin-policy.json
- AmazonMSKFullAccess
- customer-msk-admin-role.json

계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: Amazon MSK 사용에 대한 제한 사항은 무엇입니까?

Amazon MSK가 구성한 대상으로 브로커 로그를 전송하려면 AmazonMSKFullAccess 정책이 IAM 역할에 연결되어 있는지 확인합니다. 따라서 전체 액세스 권한이 이미 있습니다.

Q: Amazon MSK를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

MSK 클러스터를 생성하기 전에 해당 VPC 내에 VPC와 서브넷이 있어야 합니다. 기본적으로 AMS는 기본 [AMS VPC 생성](#)의 일부로 이를 다룹니다.

Amazon MSK의 제한에 대해 알아보려면 [Amazon MSK 제한을 참조하세요](#).

AMS SSP를 사용하여 AMS 계정에서 Amazon Managed Service for Prometheus 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Managed Service for Prometheus(AMP) 기능에 직접 액세스할 수 있습니다. Amazon Managed Service for Prometheus는 컨테이너 지표에 대한 서버리스, Prometheus 호환 모니터링 서비스로 컨테이너 환경을 대규모로 더 쉽고 안전하게 모니터링할 수 있도록 합니다. Amazon Managed Service for Prometheus를 사용하면 컨테이너화된 워크로드의 성능을 모니터링하는 데 현재 사용하는 것과 동일한 오픈 소스 Prometheus 데이터 모델과 쿼리 언어를 사용할 수 있으며, 기본 인프라를 관리할 필요 없이 향상된 확장성, 가용성 및 보안도 누릴 수 있습니다.

Amazon Managed Service for Prometheus는 워크로드가 확장 및 축소됨에 따라 운영 지표의 수집, 스토리지 및 쿼리를 자동으로 확장합니다. 보안 AWS 서비스와 통합되어 데이터에 빠르고 안전하게 액세스할 수 있습니다. 자세한 내용은 [Amazon Managed Service for Prometheus란 무엇입니까?](#)를 참조하세요.

AWS Managed Services FAQ의 AWS Managed Services for Prometheus

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Managed Service for Prometheus에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer-

prometheus-console-role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 customer-prometheus-console-role 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Managed Service for Prometheus 사용에 대한 제한 사항은 무엇인가요?

모든 기능이 지원됩니다.

Q: AMS 계정에서 Amazon Managed Service for Prometheus를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon Managed Service for Prometheus를 시작하기 위한 사전 조건이나 종속성은 없습니다. 그러나 특정 사용 사례에 따라 다른 AWS 서비스에 대한 액세스가 필요할 수 있습니다.

AMS SSP를 사용하여 AMS 계정에서 Personalize 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Personalize 기능에 액세스할 수 있습니다. Personalize는 개발자가 애플리케이션을 사용하는 고객을 위한 개별화된 추천을 쉽게 생성할 수 있는 기계 학습 서비스입니다.

기계 학습은 맞춤형 제품 및 콘텐츠 추천, 맞춤형 검색 결과, 대상 마케팅 프로모션을 강화하여 고객 참여를 개선하는 데 점점 더 많이 사용되고 있습니다. 그러나 이러한 정교한 권장 시스템을 만드는 데 필요한 기계 학습 기능을 개발하는 것은 복잡성으로 인해 오늘날 대부분의 조직의 범위를 벗어났습니다. Personalize를 사용하면 이전 기계 학습 경험이 없는 개발자가 Amazon.com 다년간 사용해 온 기계 학습 기술을 사용하여 애플리케이션에 정교한 개인화 기능을 쉽게 구축할 수 있습니다.

Personalize를 사용하면 클릭, 페이지 보기, 가입, 구매 등 애플리케이션의 활동 스트림과 기사, 제품, 비디오 또는 음악과 같이 추천하려는 항목의 인벤토리를 제공할 수 있습니다. Personalize에 연령 또는 지리적 위치와 같은 사용자의 추가 인구 통계 정보를 제공하도록 선택할 수도 있습니다. Personalize는 데이터를 처리 및 검사하고, 의미 있는 것을 식별하고, 올바른 알고리즘을 선택하고, 데이터에 맞게 사용자 지정된 개인화 모델을 훈련 및 최적화합니다. Personalize에서 분석한 모든 데이터는 비공개로 안전하게 유지되며 사용자 지정 권장 사항에만 사용됩니다. 간단한 API 직접 호출을 통해 맞춤형 추천을 제공할 수 있습니다. 사용한 만큼만 비용을 지불하며, 최소 요금이나 선결제 약정은 없습니다.

자세한 내용은 [Personalize](#)를 참조하세요.

AWS Managed Services Amazon Personalize FAQ

Q: AMS 계정에서 Personalize에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny)
변경 유형을 제출하여 액세스를 요청하고, 추천을 생성하기 위해 AWS Personalize에서 사용할

데이터가 포함된 S3 버킷을 지정해야 합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다 customer_personalize_console_role customer_personalize_service_role.

- customer_personalize_console_role가 계정에 프로비저닝되면 페더레이션 솔루션의 역할을 온보딩해야 합니다. 이외의 다른 기존 역할에 customer_personalize_console_policy를 연결할 수도 있습니다 Customer_ReadOnly_Role.
- customer_personalize_service_role가 계정에 제공되면 새 데이터 세트 그룹을 생성할 때 해당 ARN을 참조할 수 있습니다.

현재 AMS Operations는 계정에 이 서비스 역할인 도 배포합니다 aws_code_pipeline_service_role_policy.

Q: AMS 계정에서 Personalize를 사용하는 데 따르는 제한 사항은 무엇인가요?

Personalize 구성은 AMS 인프라에 대한 수정을 방지하기 위해 'ams-' 또는 'mc-' 접두사가 없는 리소스로 제한됩니다.

Q: AMS 계정에서 Personalize를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- 데이터가 저장되는 S3 버킷이 암호화된 경우 Personalize에서 사용하는 역할이 버킷을 해독하도록 허용할 수 있도록 KMS 키 ID를 제공해야 합니다.

Personalize는 기본 KMS S3 키를 지원하지 않습니다. KMS를 사용해야 하는 경우 사용자 지정 키를 생성하고 변경 유형 KMS 키 | 생성(검토 필요)이 있는 RFC를 열어 다음 정책을 추가합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy-3",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": "kms:*",
      "Resource": "*"
    }
  ]
}
```


}

- S3 버킷은 다음 버킷 정책을 사용하여 생성해야 합니다. 변경 유형 S3 스토리지 | 정책 생성이 포함된 RFC를 제출하여이 작업을 수행합니다. 이 정책은 Personalize가 데이터에 액세스할 수 있도록 허용합니다. 해당 버킷에는 Personalize에서 사용할 데이터가 포함됩니다.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PersonalizeS3BucketAccessPolicy",
  "Statement": [
    {
      "Sid": "PersonalizeS3BucketAccessPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

AMS SSP를 사용하여 AMS 계정에서 Amazon QuickSight 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 QuickSight 기능에 액세스할 수 있습니다. QuickSight는 조직의 모든 사람에게 인사이트를 제공하는 빠른 클라우드 기반 비즈니스 인텔리전스 서비스입니다. 완전관리형 서비스인 QuickSight를 사용하면 기계 학습(ML) 인사이트가 포함된 대화형 대시보드를 쉽게 생성하고 게시할 수 있습니다. 자세한 내용은 [Amazon QuickSight](#)를 참조하세요.

AWS Managed Services QuickSight FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 QuickSight에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)
를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다
customer_quicksight_console_admin_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 QuickSight를 사용할 때 제한 사항은 무엇인가요?

- AWS IAM 정책 종속성으로 인해 QuickSight의 리소스 설정에 액세스할 수 없습니다. 그러나 AMS 팀은 서비스 활성화 요청에 대한 응답으로 각 리소스를 활성화합니다.
- 이 기능을 사용하면 사용자가 AMS 인프라를 손상시킬 수 있는 IAM 권한을 변경할 수 있으므로 개별 사용자 및 그룹에 대한 리소스 액세스는 이 모델에서 지원되지 않습니다.
- QuickSight 내에서 IAM 자격 증명을 초대하는 기능은 IAM 객체 변경과 관련된 위험으로 인해 지원되지 않습니다.
- QuickSight 서비스는 Enterprise와 Standard라는 두 가지 에디션을 제공합니다. 둘 다 AMS에서 지원되는 SSO(Single Sign-On) 옵션을 제공합니다. 그러나 Enterprise Edition에는 QuickSight를 Active Directory(AD)와 통합하는 옵션이 있습니다. AMS의 QuickSight는 AMS 계정 구조와 QuickSight 신원 요구 사항 간의 비호환성으로 인해 AD와의 통합을 지원하지 않습니다.

Q: AMS 계정에서 QuickSight를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- AMS가 QuickSight를 추가하기 위해 이 RFC를 수신하면 추가 정보에 대한 서비스 요청이 전송됩니다. 다음을 제공합니다.
 - QuickSight 계정 이름(예: *CustomerName*-quicksight)
 - QuickSight Edition(Standard 및 Enterprise)
 - QuickSight 서비스를 활성화할 AWS 리전입니다(기본값은 AMS AWS 리전).
 - QuickSight 계정의 알림 이메일 주소입니다.
 - (선택 사항) 분석할 데이터 파일이 있는 S3 버킷입니다.
 - QuickSight에 연결하는 VPC 및 서브넷 IDs는 QuickSight와 계정 내 리소스 간의 프라이빗 연결을 지원하는 VPC 연결을 추가하는 기능을 지원합니다.

AMS 운영자는 사용자를 대신하여 가입 프로세스를 수행하고 두 가지 QuickSight 기능을 구성합니다.

- 데이터 소스에 대한 [자동 검색](#).
- [VPC 연결](#).

Note

로그인 프로세스 중에 승격된 IAM 및 VPC 권한이 필요하므로 AMS 운영자가 이러한 작업을 수행해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Rekognition 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Rekognition 기능에 직접 액세스할 수 있습니다. Amazon Rekognition을 사용하면 기계 학습 전문 지식이 필요 없는 확장이 뛰어난 검증된 딥 러닝 기술을 사용하여 애플리케이션에 이미지 및 비디오 분석을 쉽게 추가할 수 있습니다. Amazon Rekognition을 사용하면 이미지 및 비디오에서 객체, 사람, 텍스트, 장면 및 활동을 식별하고 부적절한 콘텐츠를 감지할 수 있습니다. 또한 Amazon Rekognition은 다양한 사용자 확인, 인원 계산 및 공공 안전 사례를 위해 얼굴을 감지, 분석 및 비교하는 데 사용할 수 있는 매우 정확한 얼굴 분석 및 얼굴 검색 기능을 제공합니다.

Amazon Rekognition Custom Labels를 사용하면 비즈니스 요구 사항에 맞는 이미지에서 객체와 장면을 식별할 수 있습니다. 예를 들어 조립 라인에서 특정 기계 부품을 분류하거나 비정상 공장을 감지하는 모델을 구축할 수 있습니다. Amazon Rekognition Custom Labels는 모델 개발 과중한 작업을 처리하므로 기계 학습 경험이 필요하지 않습니다. 식별하려는 객체 또는 장면의 이미지를 제공하면 서비스가 나머지를 처리합니다.

자세한 내용은 [Amazon Rekognition](#)을 참조하세요.

AWS Managed Services FAQ의 Amazon Rekognition

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon Rekognition에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_rekognition_console_role & customer_rekognition_service_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Rekognition을 사용할 때 제한 사항은 무엇인가요?

Amazon Rekognition의 전체 기능은 Amazon Rekognition 자체 프로비저닝된 서비스 역할에서 사용할 수 있습니다.

Q: AMS 계정에서 Amazon Rekognition을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon Rekognition Video 스트림 프로세서 또는 데이터 스트림에 대한 소스 스트리밍 비디오를 Kinesis Data Streams에 데이터를 쓸 대상으로 제공하는 Kinesis Video Streams를 사용하는 경우 RFC를 생성할 `kinesisStreamName` 때 AMS에를 제공하세요.

AMS SSP를 사용하여 AMS 계정에서 Amazon SageMaker AI 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Amazon SageMaker AI 기능에 액세스합니다. SageMaker AI는 모든 개발자와 데이터 과학자에게 기계 학습 모델을 신속하게 구축, 훈련 및 배포할 수 있는 기능을 제공합니다. Amazon SageMaker AI는 데이터에 레이블을 지정하고 준비하며, 알고리즘을 선택하고, 모델을 훈련하고, 배포를 위해 조정하고 최적화하고, 예측하고, 조치를 취하는 전체 기계 학습 워크플로를 포괄하는 완전관리형 서비스입니다. 모델은 훨씬 적은 노력과 비용으로 더 빠르게 프로덕션에 도달할 수 있습니다. 자세한 내용은 [Amazon SageMaker AI](#)를 참조하세요.

AWS Managed Services의 SageMaker AI FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 SageMaker AI에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | (ct-1w8z66n899dct) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 `customer_sagemaker_admin_role` 서비스 역할을 프로비저닝합니다. `AmazonSageMaker-ExecutionRole-Admin`. 계정에 SageMaker AI가 프로비저닝된 후 페더레이션 솔루션에서 `customer_sagemaker_admin_role` 역할을 온보딩해야 합니다. 서비스 역할은 사용자가 직접 액세스할 수 없습니다. SageMaker AI 서비스는 역할 [전달에 설명된 대로 다양한 작업을 수행하는 동안 서비스 역할을](#) 사용합니다.

Q: AMS 계정에서 SageMaker AI를 사용할 때 제한 사항은 무엇인가요?

- 다음 사용 사례는 AMS Amazon SageMaker AI IAM 역할에서 지원되지 않습니다.
 - SageMaker AI Studio는 현재 지원되지 않습니다.
 - 프라이빗 작업 인력을 관리하기 위한 SageMaker AI Ground Truth는 지원되지 않습니다. 이 기능을 사용하려면 Amazon Cognito 리소스에 대한 지나치게 허용적인 액세스가 필요하기 때문입니다. 프라이빗 작업 인력을 관리해야 하는 경우 SageMaker AI 및 Amazon Cognito 권한이 결합된 사용자 지정 IAM 역할을 요청할 수 있습니다. 그렇지 않으면 데이터 레이블 지정에 퍼블릭 작업 인력(Amazon Mechanical Turk 지원) 또는 AWS Marketplace 서비스 공급자를 사용하는 것이 좋습니다.
- SageMaker AI 서비스(`aws.sagemaker.{region}.notebook`, `com.amazonaws.{region}.sagemaker.api` & `com.amazonaws.{region}.sagemaker.runtime`)에 대한 API 호출을 지원하는 VPC 엔드포인트 생성

은 SageMaker AI 관련 서비스로만 권한 범위를 지정할 수 없으므로 지원되지 않습니다. 이 사용 사례를 지원하려면 관리 | 기타 | 기타 RFC를 제출하여 관련 VPC 엔드포인트를 생성합니다.

- SageMaker AI에는 모든 ("") 리소스에 대한 DeleteAlarm 권한이 필요하므로 SageMaker AI 엔드포인트 Auto Scaling은 지원되지 않습니다. 엔드포인트 Auto Scaling을 지원하려면 Management | Other | Other RFC를 제출하여 SageMaker AI 엔드포인트에 대한 Auto Scaling을 설정합니다.

Q: AMS 계정에서 SageMaker AI를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- 다음 사용 사례에서는 사용 전에 특별한 구성이 필요합니다.
 - S3 버킷을 사용하여 모델 아티팩트와 데이터를 저장하는 경우 배포 | 고급 스택 구성 요소 | S3 스토리지 | RFC 생성과 함께 필수 키워드("SageMaker", "Sagemaker", "sagemaker" 또는 "aws-glue")가 포함된 라는 S3 버킷을 요청해야 합니다.
 - Elastic File Store(EFS)를 사용할 경우 EFS 스토리지를 동일한 서브넷에 구성하고 보안 그룹에서 허용해야 합니다.
 - 다른 리소스가 SageMaker AI 서비스(노트북, API, 런타임 등)에 직접 액세스해야 하는 경우 다음을 통해 구성을 요청해야 합니다.
 - RFC를 제출하여 엔드포인트에 대한 보안 그룹 생성(배포 | 고급 스택 구성 요소 | 보안 그룹 | 생성(자동)).
 - 관리 제출 | 기타 | 기타 | RFC를 생성하여 관련 VPC 엔드포인트를 설정합니다.

Q:가 직접 액세스할 **customer_sagemaker_admin_role** 수 있는 리소스에 대해 지원되는 이름 지정 규칙은 무엇입니까? (다음은 업데이트 및 삭제 권한을 위한 것입니다. 리소스에 지원되는 추가 명명 규칙이 필요한 경우 AMS Cloud Architect에 문의하여 상담을 받으세요.)

- 리소스: AmazonSageMaker-ExecutionRole-* 역할 전달
 - 권한: SageMaker AI 자체 프로비저닝된 서비스 역할은 AWS Glue AWS RoboMaker 및와 함께 SageMaker AI 서비스 역할(AmazonSageMaker-ExecutionRole-*)을 사용할 수 있도록 지원합니다 AWS Step Functions.
- 리소스: Secrets Manager의 AWS 보안 암호
 - 권한: AmazonSageMaker-* 접두사를 사용하여 보안 암호를 설명, 생성, 가져오기, 업데이트합니다.
 - 권한: SageMaker 리소스 태그가 로 설정된 경우 설명, 보안 암호 가져오기true.
- 리소스:의 리포지토리 AWS CodeCommit
 - 권한: AmazonSageMaker-* 접두사가 있는 리포지토리를 생성/삭제합니다.

- 권한: 접두사 , *sagemaker*, *SageMaker*가 있는 리포지토리의 Git Pull/Push*Sagemaker*.
- 리소스: Amazon ECR(Amazon Elastic Container Registry) 리포지토리
 - 권한: 권한: 다음 리소스 이름 지정 규칙인을 사용할 때 리포지토리 정책을 설정, 삭제 및 컨테이너 이미지를 업로드합니다*sagemaker*.
- 리소스: Amazon S3 버킷
 - 권한: 리소스에 , *Sagemaker* *sagemaker* 및 접두사가 있는 경우 객체 가져오기, 넣기*SageMaker*, 삭제, 멀티파트 업로드 S3 객체 중단aws-glue.
 - 권한: SageMaker 태그가 로 설정된 경우 S3 객체를 가져옵니다true.
- 리소스: Amazon CloudWatch 로그 그룹
 - 권한: 로그 그룹 또는 스트림 생성, 로그 이벤트 넣기, 나열, 업데이트, 생성, 접두사가 있는 로그 전송 삭제/aws/sagemaker/*.
- 리소스: Amazon CloudWatch 지표
 - 권한: , AWS/SageMaker, , AWS/SageMaker/, aws/SageMaker, 및 접두사가 사용되는 경우 지표 데이터를 넣습니다aws/SageMaker/aws/sagemakeraws/sagemaker//aws/sagemaker/..
- 리소스: Amazon CloudWatch Dashboard
 - 권한: 접두사가 사용될 때 대시보드를 생성/삭제합니다customer_*.
- 리소스: Amazon SNS(Simple Notification Service) 주제
 - 권한: *sagemaker*, *SageMaker*및 접두사가 사용되는 경우 주제를 구독/생성합니다*Sagemaker*.

Q: AmazonSageMakerFullAccess와의 차이점은 무엇인가
요customer_sagemaker_admin_role?

를 customer_sagemaker_admin_role 사용하는는 다음을 제외하고 AmazonSageMakerFullAccess와 거의 동일한 권한을 customer_sagemaker_admin_policy 제공합니다.

- AWS RoboMaker에 연결할 수 있는 권한, Amazon Cognito 및 AWS Glue 리소스.
- SageMaker AI 엔드포인트 자동 크기 조정. Autoscaling에는 CloudWatch 서비스에 대한 허용적 액세스가 필요하므로 관리 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 엔터티 또는 정책 업데이트(검토 필요) 변경 유형(ct-27tuth19k52b4)을 사용하여 RFC를 제출하여 Autoscaling 권한을 임시 또는 영구적으로 승격해야 합니다.

Q: 유휴 데이터 암호화에 AWS KMS 고객 관리형 키를 채택하려면 어떻게 해야 하나요?

관련 IAM 사용자 또는 역할이 키를 사용할 수 있도록 고객 관리형 키에 키 정책이 올바르게 설정되었는지 확인해야 합니다. 자세한 내용은 [AWS KMS 키 정책 문서를](#) 참조하세요.

AMS SSP를 사용하여 AMS 계정에서 Amazon Simple Email Service 프로비저닝

AMS 자체 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Simple Email Service(Amazon SES) 기능에 직접 액세스할 수 있습니다. Amazon Simple Email Service는 디지털 마케팅과 애플리케이션 개발자가 마케팅, 알림 및 트랜잭션 이메일을 보낼 수 있도록 설계된 클라우드 기반 이메일 전송 서비스입니다.

SMTP 인터페이스 또는 AWS SDKs 중 하나를 사용하여 Amazon SES를 기존 애플리케이션에 직접 통합할 수 있습니다. 또한 Amazon SES의 이메일 전송 기능을 티켓팅 시스템 및 이메일 클라이언트와 같이 이미 사용 중인 소프트웨어에 통합할 수 있습니다.

자세한 내용은 [Amazon Simple Email Service](#)를 참조하세요.

AWS Managed Services의 Amazon SES FAQ

Q: AMS 계정에서 Amazon SES에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Amazon SES에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_ses_admin_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon SES를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- Amazon SES가 버킷에 이벤트를 게시할 수 있도록 S3 버킷 정책을 구성해야 합니다.
- Amazon AWS SES가 계정에 속한 Amazon S3, Amazon SES)을 사용하거나 CMK 키를 구성해야 합니다. Amazon SNS

Q: AMS 계정에서 Amazon SES를 사용할 때 제한 사항은 무엇인가요?

다음 리소스를 생성하려면 RFCs를 생성해야 합니다.

- Kinesis Firehose 스트림에 대한 PutEvents 권한이 있는 SMTP 사용자 및 IAM 서비스 역할.

- Amazon SES 규칙 및 구성 세트의 대상이 해당 AWS 리소스와 함께 작동하려면 AMS 변경 유형을 사용하여 S3 버킷, Firehose 스트림, SNS 주제와 같은 새 리소스를 생성해야 합니다.
- SMTP 자격 증명. 새 SMTP 자격 증명을 요청하려면 변경 유형(관리 | 기타 | 기타 | 생성)을 사용합니다. AMS는 자격 증명을 생성하여 Secrets Manager에 추가합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Simple Workflow Service 프로비저닝

AMS 자체 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Simple Workflow Service(Amazon SWF) 기능에 직접 액세스할 수 있습니다. Amazon Simple Workflow Service는 개발자가 병렬 또는 순차적 단계가 있는 백그라운드 작업을 빌드, 실행 및 확장하는 데 도움이 됩니다. Amazon SWF를 클라우드에서 완전 관리형 상태 트래커 및 작업 코디네이터로 생각할 수 있습니다. 애플리케이션의 단계를 완료하는 데 500밀리초 이상 걸리거나 처리 상태를 추적해야 하거나 작업이 실패할 경우 복구 또는 재시도해야 하는 경우 Amazon SWF가 도와드릴 수 있습니다. 자세한 내용은 [Amazon Simple Workflow Service](#)를 참조하세요.

AWS Managed Services의 Amazon SWF FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Amazon SWF에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_swf_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon SWF를 사용할 때 제한 사항은 무엇인가요?

Lambda InvokeFunction 권한은이 서비스에 포함되어 있지만 모든 AMS 고객 역할에 추가된 AMScustomer_deny_policy는 AMS Lambda 함수 및 AMS 소유 리소스에 대한 액세스를 명시적으로 거부합니다. Amazon SWF 내에서 리소스에 태그를 지정하거나 태그를 해제하려면 관리 | 기타 | 기타 변경 유형을 제출합니다.

Q: AMS 계정에서 Amazon SWF를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Amazon SWF는 AWS Lambda 서비스에 종속되므로이 역할의 일부로 Lambda를 호출할 수 있는 권한이 제공되었으며 Amazon SWF에서 Lambda를 호출하는 데 추가 권한이 필요하지 않습니다. 그렇지 않으면 Amazon SWF를 사용하기 위한 사전 조건이 없습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Textract 프로비저닝

AMS 자체 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Textract 기능에 직접 액세스할 수 있습니다. Amazon Textract는 간단한 광학 문자 인식(OCR)을 넘어 양식 및 테이블에서 데이터를 식별, 이해 및 추출하는 스캔한 문서에서 인쇄된 텍스트, 필기 및 기타 데이터를 자동으로 추출하는 완전관리형 기계 학습 서비스입니다. 자세한 내용은 [Amazon Textract](#)를 참조하세요.

AWS Managed Services FAQ의 Amazon Textract

일반적인 질문과 답변:

Q: Amazon Textract를 AMS 계정에 설정하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 `customer_textract_console_role`, `customer_textract_human_review_execution_role` 및 IAM 역할을 프로비저닝합니다. `customer_ec2_textract_instance_profile`. 계정에 프로비저닝된 후에는 페더레이션 솔루션 `customer_textract_console_role`의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Textract를 사용할 때 제한 사항은 무엇인가요?

AMS 계정에서 Amazon Textract를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 Amazon Textract를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

RFC 배포 | 고급 스택 구성 요소 | S3 스토리지 | 생성(ct-1a68ck03fn98r)을 제출하여 S3 버킷 생성을 요청해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon Transcribe 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Amazon Transcribe 기능에 직접 액세스할 수 있습니다. Amazon Transcribe는 오디오 파일에서 타임스탬프가 지정된 텍스트 트랜스크립트를 자동으로 생성하는 완전 관리형이며 지속적으로 훈련된 자동 음성 인식 서비스입니다. Amazon Transcribe를 사용하면 개발자가 애플리케이션에 speech-to-text 변환 기능을 쉽게 추가할 수 있습니다. 컴퓨터가 오디오 데이터를 검색하고 분석하는 것은 사실상 불가능합니다. 따라서 애플리케이션에서 사용하기 전에 녹음된 음성을 텍스트로 변환해야 합니다. 과거에는 고객이 값비싼 계약에 서명해야 하고 이 작업을 수행하기 위해 기술 스택에 통합하기 어려운 트랜스크립션 공급자와 협력해야 했습니다. 이러한 공급자 중 다수는 콜센터에서 흔히 사용되는 저충실도 전화 오디오와 같은 다양한 시나리오에 잘 적응하지 못하는 오래된 기술을 사용하므로 정확도가 떨어집니다.

Amazon Transcribe는 자동 음성 인식(ASR)이라는 딥 러닝 프로세스를 사용하여 음성을 텍스트로 빠르고 정확하게 변환합니다. Amazon Transcribe를 사용하여 고객 서비스 호출을 트랜스크립션하고, 자막 및 자막을 자동화하고, 미디어 자산에 대한 메타데이터를 생성하여 완전히 검색 가능한 아카이브를 생성할 수 있습니다. Amazon Transcribe Medical을 사용하여 임상 문서 애플리케이션에 의료 speech-to-text 기능을 추가할 수 있습니다. 자세한 내용은 [Amazon Transcribe](#)를 참조하세요.

AWS Managed Services FAQ의 Amazon Transcribe

일반적인 질문과 답변:

Q: Amazon Transcribe를 AMS 계정에 설정하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_transcribe_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Amazon Transcribe를 사용할 때 제한 사항은 무엇인가요?

RA 밑에서 달리 지정하지 않는 한 트랜스크립션 작업 시 버킷의 접두사로 'customer-transcribe*'를 사용해야 합니다.

Amazon 트랜스크립션 내에서 IAM 역할을 생성할 수 없습니다.

기본 SSPS의 출력 데이터에 서비스 관리형 S3 버킷을 사용할 수 없습니다(필요한 경우 계정 CA에 문의).

AMS 네임스페이스에 속하지 않는 고객 관리형 KMS 키를 사용하려면 위험 승인을 제출해야 합니다.

Q: AMS 계정에서 Amazon Transcribe를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

S3에는 이름이 'customer-transcribe*'인 버킷에 대한 액세스 권한이 있어야 합니다. S3 버킷이 KMS 키로 암호화된 경우 Amazon Transcribe를 사용하려면 KMS가 필요합니다. 버킷을 암호화할 필요가 없는 경우 "KMStranscribeAllow"를 제거할 수 있습니다.

AMS SSP를 사용하여 AMS 계정에서 Amazon WorkSpaces 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 WorkSpaces 기능에 직접 액세스할 수 있습니다. WorkSpaces를 사용하면 사용자를 위해 WorkSpaces라고 하는 가상 클라우드 기반 Microsoft Windows 또는 Amazon Linux 데스크톱을 프로비저닝할 수 있습니다. WorkSpaces를 사용하면 하드웨어를 구매하고 배포하거나 복잡한 소프트웨어를 설치할 필요가 없습니다. 필요에 따라 신속하게 사용자를 추가 또는 제거할 수 있습니다. 사용자는 지원되는 디바이스의 클라이언트 애플

리케이션을 사용하거나 Windows WorkSpaces의 경우 웹 브라우저를 사용하여 WorkSpaces에 액세스하고 기존 온프레미스 Active Directory(AD) 자격 증명을 사용하여 로그인합니다.

자세한 내용은 [Amazon WorkSpaces](#) 참조하세요.

AWS Managed Services FAQ의 WorkSpaces

일반적인 질문과 답변:

Q: AMS 계정에서 WorkSpaces에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_workspaces_console_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 WorkSpaces 사용에 대한 제한 사항은 무엇인가요?

Workspaces의 전체 기능은 Amazon WorkSpaces 자체 프로비저닝된 서비스 역할에서 사용할 수 있습니다.

Q: AMS 계정에서 WorkSpaces를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- WorkSpaces는 AWS 리전별로 제한되므로 WorkSpaces 인스턴스가 호스팅되는 리전과 동일한 AWS 리전에서 AD 커넥터를 구성해야 합니다.

고객은 다음 두 가지 방법 중 하나를 사용하여 WorkSpaces를 고객 AD에 연결할 수 있습니다.

1. AD 커넥터를 사용하여 온프레미스 Active Directory 서비스에 대한 인증 프록시(선호됨):

WorkSpaces 인스턴스를 온프레미스 디렉터리 서비스와 통합하기 전에 AMS 계정에서 Active Directory(AD) 커넥터를 구성합니다. AD 커넥터는 기존 AD 사용자(도메인)가 기존 온프레미스 AD 자격 증명을 사용하여 WorkSpaces에 연결하는 프록시 역할을 합니다. 이는 WorkSpaces가 리소스 포리스트와 사용자 포리스트 역할을 하는 고객의 온프레미스 도메인에 직접 조인되어 고객 측에서 더 많은 제어를 할 수 있기 때문에 선호됩니다.

자세한 내용은 [Amazon WorkSpaces 배포 모범 사례\(시나리오 1\)](#)를 참조하세요.

2. AWS Microsoft AD, 공유 서비스 VPC 및 온프레미스에 대한 단방향 신뢰와 함께 AD Connector 사용:

또한 먼저 AMS 관리형 AD에서 온프레미스 AD로의 단방향 발신 신뢰를 구축하여 온프레미스 디렉터리로 사용자를 인증할 수 있습니다. WorkSpaces는 AD 커넥터를 사용하여 AMS 관리형 AD

를 조인합니다. 그러면 온프레미스 환경과 양방향 신뢰를 구축할 필요 없이 AMS 관리형 AD를 통해 WorkSpaces 액세스 권한이 WorkSpaces 인스턴스에 위임됩니다. 이 시나리오에서 사용자 포리스트는 고객 AD에 있고 리소스 포리스트는 AMS 관리형 AD에 있습니다(AMS 관리형 AD에 대한 변경은 RFC를 통해 요청할 수 있음). WorkSpaces VPC와 AMS 관리형 AD를 실행하는 MALZ 공유 서비스 VPC 간의 연결은 Transit Gateway를 통해 설정됩니다.

자세한 내용은 [Amazon WorkSpaces 배포 모범 사례\(시나리오 6\)](#)를 참조하세요.

Note

AD 커넥터는 사전 필수 AD 구성 세부 정보가 포함된 관리 | 기타 | 기타 | 변경 유형 생성 RFC를 제출하여 구성할 수 있습니다. 자세한 내용은 [AD 커넥터 생성을 참조하세요](#). 메서드 2를 사용하여 AMS 관리형 AD에서 리소스 포리스트를 생성하는 경우 AMS 관리형 AD를 실행하여 AMS 공유 서비스 계정에서 다른 관리 | 기타 | 기타 | 변경 유형 RFC를 제출하세요.

AMS SSP를 사용하여 AMS 계정에서 AMS 코드 서비스 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AMS Code 서비스 기능에 직접 액세스할 수 있습니다. AMS 코드 서비스는 다음에 자세히 설명된 AWS 코드 관리 서비스의 독점 번들링입니다. AMS Code 서비스와 함께 AMS에 모든 서비스를 배포하도록 선택하거나 AMS에 개별적으로 배포할 수 있습니다.

AMS 코드 서비스에는 다음 서비스가 포함됩니다.

- AWS CodeCommit: 보안 Git 기반 리포지토리를 호스팅하는 완전 관리형 [소스 제어](#) 서비스입니다. 이를 통해 팀은 안전하고 확장성이 뛰어난 에코시스템에서 코드에 대해 협업할 수 있습니다. CodeCommit을 사용하면 자체 소스 제어 시스템을 운영하거나 인프라 규모 조정에 대해 걱정할 필요가 없습니다. CodeCommit을 사용하여 소스 코드에서 바이너리에 이르기까지 모든 것을 안전하게 저장할 수 있으며 기존 Git 도구와 원활하게 작동합니다. 자세한 내용은 [AWS CodeCommit](#) 섹션을 참조하세요.

AMS Code 서비스와 독립적으로 AMS 계정에 이를 배포하려면 섹션을 참조하세요 [AMS SSP를 사용하여 AMS 계정 AWS CodeCommit 에서 프로비저닝](#).

- AWS CodeBuild: 소스 코드를 컴파일하고, 테스트를 실행하고, 배포할 준비가 된 소프트웨어 패키지를 생성하는 완전 관리형 지속적 통합 서비스입니다. CodeBuild를 사용하면 자체 빌드 서버를 프로비저닝, 관리 및 조정할 필요가 없습니다. CodeBuild는 지속적으로 규모가 조정되며 여러 빌드를 동시에 처리하기 때문에 빌드가 대기열에서 대기하지 않고 바로 처리됩니다. 사전 패키징된 빌드 환경

을 사용하면 신속하게 시작할 수 있으며 혹은 자체 빌드 도구를 사용하는 사용자 지정 빌드 환경을 만들 수 있습니다. CodeBuild를 사용하면 컴퓨팅 리소스에 대한 분당 사용 요금이 청구됩니다. 자세한 내용은 [AWS CodeBuild](#) 섹션을 참조하세요.

AMS Code 서비스와 독립적으로 AMS 계정에 이를 배포하려면 섹션을 참조하세요 [AMS SSP를 사용하여 AMS 계정 AWS CodeBuild 에서 프로비저닝](#).

- AWS CodeDeploy: Amazon EC2 및 온프레미스 서버와 같은 다양한 컴퓨팅 서비스에 대한 소프트웨어 배포를 자동화하는 완전관리형 배포 서비스입니다. AWS CodeDeploy 를 사용하면 새 기능을 신속하게 릴리스하고, 애플리케이션 배포 중에 가동 중지를 방지하고, 애플리케이션 업데이트의 복잡성을 처리할 수 있습니다. AWS CodeDeploy 를 사용하여 소프트웨어 배포를 자동화할 수 있으므로 오류가 발생하기 쉬운 수동 작업이 필요하지 않습니다. 서비스는 배포 요구 사항에 맞게 확장됩니다. 자세한 내용은 [AWS CodeDeploy](#) 섹션을 참조하세요.

AMS Code 서비스와 독립적으로 AMS 계정에 이를 배포하려면 섹션을 참조하세요 [AMS SSP를 사용하여 AMS 계정 AWS CodeDeploy 에서 프로비저닝](#).

- AWS CodePipeline: 빠르고 안정적인 애플리케이션 및 인프라 업데이트를 위해 릴리스 파이프라인을 자동화하는 데 도움이 되는 완전 관리형 [지속적 제공](#) 서비스입니다. CodePipeline은 정의한 릴리스 모델을 기반으로 코드 변경이 있을 때마다 릴리스 프로세스의 구축, 테스트 및 배포 단계를 자동화합니다. 이를 통해 기능과 업데이트를 신속하고 안정적으로 제공할 수 있습니다. GitHub AWS CodePipeline 와 같은 타사 서비스 또는 자체 사용자 지정 플러그인과 쉽게 통합할 수 있습니다. AWS CodePipeline에서는 사용한 만큼만 비용을 지불합니다. 선수금이나 장기 약정을 적용하지 않습니다. 자세한 내용은 [AWS CodePipeline](#) 섹션을 참조하세요.

AMS Code 서비스와 독립적으로 AMS 계정에 이를 배포하려면 섹션을 참조하세요 [AMS SSP를 사용하여 AMS 계정 AWS CodePipeline 에서 프로비저닝](#).

AWS Managed Services FAQ의 AMS 코드 서비스

Q: 내 AMS 계정의 AMS 코드 서비스에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_code_suite_console_role. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다. 현재 AMS Operations는 CodeBuildcustomer_codebuild_service_role, CodeDeploy 및 CodePipeline CodePipeline customer_codedeploy_service_role aws_code_pipeline_service_role 서

비스에 대한 계정에 , , 서비스 역할도 배포합니다. CodeBuild 에 대한 추가 IAM 권한이 customer_codebuild_service_role 필요한 경우 AMS 서비스 요청을 제출합니다.

Note

이러한 서비스를 별도로 추가할 수도 있습니다. 자세한 내용은 [AMS SSP를 사용하여 AMS 계정 AWS CodePipeline 에서 프로비저닝](#) 각각 [AMS SSP를 사용하여 AMS 계정 AWS CodeBuild 에서 프로비저닝](#), [AMS SSP를 사용하여 AMS 계정 AWS CodeDeploy 에서 프로비저닝](#) 및 단원을 참조하십시오.

Q: AMS 계정에서 AMS 코드 서비스를 사용할 때 제한 사항은 무엇인가요?

- AWS CodeCommit: SNS 주제를 생성할 수 있는 관련 권한이 주어진다면 CodeCommit의 트리거 기능이 비활성화됩니다. CodeCommit에 대한 직접 인증은 제한되므로 사용자는 자격 증명 헬퍼로 인증해야 합니다. kms:Encrypt, kms:Decrypt, kms:ReEncrypt, kms:GenerateDataKey, kms:GenerateDataKeyWithoutPlaintext, kms:DescribeKey 등의 일부 KMS 명령도 제한됩니다.
- CodeBuild: AWS CodeBuild 콘솔 관리자 액세스의 경우 리소스 수준에서 권한이 제한됩니다. 예를 들어 CloudWatch 작업은 특정 리소스로 제한되고 iam:PassRole 권한은 제어됩니다.
- CodeDeploy: 현재 CodeDeploy는 Amazon EC2/온프레미스에서만 배포를 지원합니다. CodeDeploy를 통한 ECS 및 Lambda 배포는 지원되지 않습니다.
- CodePipeline: CodePipeline 기능, 단계 및 공급자는 다음으로 제한됩니다.
 - 배포 단계: Amazon S3 및 AWS CodeDeploy
 - 소스 단계: Amazon S3, AWS CodeCommit, 비트 버킷 및 GitHub
 - 빌드 단계: AWS CodeBuild 및 Jenkins
 - 승인 단계: Amazon SNS
 - 테스트 단계: AWS CodeBuild, Jenkins, BlazeMeter, Ghost Inspector UI Testing, Micro Focus StormRunner Load, Runscope API Monitoring
 - 호출 단계: Step Functions 및 Lambda

Note

AMS Operations는 계정에 customer_code_pipeline_lambda_policy를 배포합니다. 이는 Lambda 간접 호출 단계에 대한 Lambda 실행 역할에 연결되어야 합니다. 이 정책을 추가할 Lambda 서비스/실행 역할 이름을 입력합니다. 사용자 지정 Lambda 서비스/실행 역할이 없는 경우 AMS는와 customer_lambda_basic_execution_role 함께의 사

본 `customer_code_pipeline_lambda_execution_role`인 라는 새 역할을 생성합니다 `customer_code_pipeline_lambda_policy`.

Q: AMS 계정에서 AMS 코드 서비스를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- CodeCommit: S3 버킷이 AWS KMS 키로 암호화된 경우 S3 AWS KMS 를 사용해야 합니다 AWS CodeCommit.
- CodeBuild: 정의된 AWS CodeBuild 서비스 역할에 추가 IAM 권한이 필요한 경우 AMS 서비스 요청을 통해 요청합니다.
- CodeDeploy: 없음.
- CodePipeline: None. AWS supported services—AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy—는 CodePipeline 시작 전 또는 이와 함께 시작해야 합니다. 그러나 이는 AMS 엔지니어가 수행합니다.

AMS SSP를 사용하여 AMS 계정 AWS Amplify 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AWS Amplify 기능에 직접 액세스할 수 있습니다. AWS Amplify 는 프론트엔드 웹 및 모바일 개발자가 풀스택 애플리케이션을 쉽게 빌드, 연결 및 호스팅할 수 있는 완벽한 솔루션입니다. Amplify는 사용 사례가 발전함에 따라 다양한 AWS 서비스를 활용할 수 있는 유연성을 제공합니다. Amplify는 풀스택 iOS, Android, Flutter, Web 및 React Native 앱을 빌드하는 제품을 제공합니다. 자세한 내용은 [AWS Amplify](#)를 참조하세요.

AWS Amplify AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정에 설정 AWS Amplify 하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 `customer_amplify_console_role`. 계정에 프로비저닝한 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

또한 에는 인프라 변경 권한이 있으므로 위험 수락 AWS Amplify 을 제공해야 합니다. 이렇게 하려면 Cloud Service Delivery Manager(CSDM)로 작업하세요.

Q: AMS 계정 AWS Amplify 에서 사용에 대한 제한 사항은 무엇인가요?

RA 밑에서 달리 지정하지 않는 한 Amplify로 작업할 때 버킷의 접두사 'amplify*' 로를 사용해야 합니다.

Q: AMS 계정 AWS Amplify 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS Amplify 에서를 사용하기 위한 사전 조건은 없습니다.

Malz 환경만 해당: Amplify의 기본 온보딩 역할은 "customer_amplify_console_role"입니다. 사용자 지정 역할을 사용하려면 먼저 IAM 엔터티를 배포합니다. 그런 다음 추가 RFC를 생성하여 애플리케이션 계정에 대한 서비스 제어 정책 허용 목록에 사용자 지정 역할을 추가합니다.

AMS SSP를 사용하여 프로비저닝 AWS AppSync

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS AppSync 기능에 액세스할 수 있습니다.는 유연한 API를 생성하여 하나 이상의 데이터 소스에서 데이터에 안전하게 액세스, 조작 및 결합할 수 있도록 함으로써 애플리케이션 개발을 간소화 AWS AppSync 합니다. AWS AppSync 는 애플리케이션이 필요한 데이터를 쉽게 가져올 수 있도록 GraphQL을 사용하는 관리형 서비스입니다.

AWS AppSync를 사용하면 NoSQL 데이터 스토어, 관계형 데이터베이스, HTTP APIs 및 사용자 지정 데이터 소스와 같은 다양한 데이터 소스에서 실시간 업데이트가 필요한 애플리케이션을 포함하여 확장 가능한 애플리케이션을 구축할 수 있습니다 AWS Lambda. 모바일 및 웹 앱의 경우는 디바이스가 오프라인 상태가 되면 로컬 데이터 액세스를 제공하고, 다시 온라인 상태가 되면 사용자 지정 가능한 충돌 해결을 통한 데이터 동기화를 AWS AppSync 제공합니다. 자세한 내용은 [AWS AppSync](#)를 참조하세요.

AWS AppSync AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS AppSync 에서 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다 customer_appsync_service_rolecustomer_appsync_author_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션customer_appsync_author_role에서 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS AppSync?

- AppSync에서 데이터 소스를 생성할 때 고객은 이전에 생성한 서비스 역할을 지정해야 하며, 새 역할 생성은 허용되지 않으므로 액세스 거부를 반환합니다.

- AppSync 역할은 AMS 인프라에 대한 수정을 방지하기 위해 'AMS-' 또는 'MC-' 접두사를 포함하는 리소스로 권한을 제한하도록 구성됩니다.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS AppSync?

서비스는 여러 다른 서비스를 데이터 소스로 사용할 수 있도록 허용합니다. 이러한 서비스를 사용할 수 있는 기본 권한은 서비스 역할(customer_appsync_service_role)에 포함되지만 서비스를 사용할 때 서비스 역할을 수동으로 선택해야 합니다.

AMS SSP를 사용하여 AMS 계정 AWS App Mesh 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS App Mesh 기능에 액세스할 수 있습니다. 애플리케이션 수준 네트워킹을 AWS App Mesh 제공하여 서비스가 여러 유형의 컴퓨팅 인프라에서 서로 쉽게 통신할 수 있도록 합니다. App Mesh는 서비스가 통신하는 방식을 표준화하여 end-to-end 가시성을 제공하고 애플리케이션의 고가용성을 보장합니다.

AWS App Mesh 를 사용하면 여러 유형의 컴퓨팅 인프라에 구축된 서비스에 대한 일관된 가시성과 네트워크 트래픽 제어를 제공하여 서비스를 쉽게 실행할 수 있습니다. App Mesh를 사용하면 애플리케이션 코드를 업데이트하여 모니터링 데이터가 수집되거나 서비스 간에 트래픽이 라우팅되는 방식을 변경할 필요가 없습니다. App Mesh는 모니터링 데이터를 내보내도록 각 서비스를 구성하고 애플리케이션 전체에서 일관된 통신 제어 로직을 구현합니다. 따라서 오류의 정확한 위치를 빠르게 파악하고 장애가 발생하거나 코드 변경을 배포해야 할 때 네트워크 트래픽을 자동으로 다시 라우팅할 수 있습니다. 자세한 내용은 [AWS App Mesh](#)를 참조하세요.

AWS App Mesh AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS App Mesh 에서 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_app_mesh_console_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS App Mesh?

의 전체 기능은 AMS 계정에서 AWS App Mesh 사용할 수 있습니다.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS App Mesh?

AMS 계정 AWS App Mesh 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Audit Manager 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Audit Manager 기능에 액세스합니다. Audit Manager를 사용하면 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 평가하는 방법을 간소화할 수 있습니다. Audit Manager는 증거 수집을 자동화하여 정책, 절차 및 활동이 효과적으로 운영되는지 더욱 쉽게 평가할 수 있도록 합니다. 감사 시기가 되면 Audit Manager는 제어에 대한 이해관계자 검토를 관리하고 수동 작업을 크게 줄이면서 감사 준비 보고서를 작성하는 데 도움이 됩니다. 자세한 내용은 [Audit Manager](#)를 참조하세요.

AWS Audit Manager AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Audit Manager 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AWS 서비스 RFC 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 제출을 통해 액세스를 요청할 수 있습니다. 이 RFC는 계정에서 다음 IAM 역할을 프로비저닝합니다. `customer-audit-manager-admin-Role`. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS Audit Manager?

AMS 계정 AWS Audit Manager 에서를 사용하는 데는 제한이 없습니다. AWS Audit Manager 에 대한 전체 기능이 제공됩니다.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS Audit Manager?

1. 보고서/평가가 상주할 s3 버킷을 AMS에 제공해야 합니다.
2. 서비스로 암호화를 사용하려면 사용할 KMS CMK ARN을 AMS에 제공해야 합니다.
3. 주제에 SNS 알림을 보내려면 주제 또는 arn의 이름을 제공해야 합니다.
4. (선택 사항) Audit Manager에서 다중 계정 랜딩 존의 일부로 Organizations를 활성화하고 위임된 관리자 계정을 원하는 경우 추가 사전 요구 사항이 있습니다. RFC(관리 | AWS 서비스 | 호환 서비스 | 추가)에 대한 설명 필드에서 위임된 관리자 계정을 Audit Manager 설정의 일부로 사용하고 아래 세부 정보를 제공하려고 한다고 언급합니다.
 - KMS CMK ARN(처음에 Audit Manager를 설정하는 데 사용됨)
 - Audit Manager가 다중 계정 랜딩 존의 일부로 사용할 수 있는 위임된 관리자 계정 ID(MALZ 애플리케이션 계정일 수 있음)

AMS SSP를 사용하여 AMS 계정 AWS Batch 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Batch 기능에 액세스할 수 있습니다. 개발자, 과학자 및 엔지니어가 수십만 개의 배치 컴퓨팅 작업을 쉽고 효율적으로 실행할 수 AWS Batch 있습니다 AWS.는 제출된 배치 작업의 볼륨 및 특정 리소스 요구 사항에 따라 최적의 수량과 유형의 컴퓨팅 리소스(예: CPU 또는 메모리 최적화 인스턴스)를 AWS Batch 동적으로 프로비저닝합니다. 를 사용하면 작업을 실행하는 데 사용하는 배치 컴퓨팅 소프트웨어 또는 서버 클러스터를 설치하고 관리할 AWS Batch필요가 없으므로 결과를 분석하고 문제를 해결하는 데 집중할 수 있습니다. 자세한 내용은 [AWS Batch](#)를 참조하세요.

AWS Batch AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Batch 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

1. 액세스를 요청하려면 RFC 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가 (ct-1w8z66n899dct)를 AWS Batch제출합니다. 이 RFC는 계정에서 다음과 같은 IAM 역할 및 정책을 프로비저닝합니다.

IAM 역할:

- customer_batch_console_role
- customer_batch_ecs_instance_role
- customer_batch_events_service_role
- customer_batch_service_role
- customer_batch_ecs_task_role

정책:

- customer_batch_console_role_policy
- customer_batch_service_role_policy
- customer_batch_events_service_role_policy

2. 계정에 프로비저닝한 후에는 페더레이션 솔루션customer_batch_console_role의 역할을 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS Batch?

컴퓨팅 환경을 생성할 때 EC2 인스턴스에 "customer_batch" 또는 "customer-batch"로 태그를 지정해야 합니다. 인스턴스에 태그가 지정되지 않은 경우 작업이 완료되면 인스턴스가 일괄적으로 종료되지 않습니다.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS Batch?

AMS 계정 AWS Batch 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Certificate Manager 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Certificate Manager (ACM) 기능에 액세스합니다. AWS Certificate Manager 는 서비스 및 내부 연결 리소스와 함께 사용할 퍼블릭 및 프라이빗 Secure Sockets Layer/Transport Layer Security(SSL/TLS) 인증서를 프로비저닝, 관리 및 배포할 수 있는 AWS 서비스입니다. SSL/TLS 인증서는 네트워크 통신을 보호하고 인터넷을 통한 웹 사이트 및 프라이빗 네트워크의 리소스의 ID를 설정하는 데 사용됩니다. SSL/TLS 인증서를 구매, 업로드 및 갱신하는 데 시간이 많이 걸리는 수동 프로세스를 AWS Certificate Manager 제거합니다.

를 사용하면 인증서를 요청하고, Elastic Load Balancer, Amazon CloudFront 배포 및 APIs Gateway의 API와 같은 ACM 통합 AWS 리소스에 배포하고,가 인증서 갱신을 AWS Certificate Manager 처리하도록 AWS Certificate Manager할 수 있습니다. 또한 내부 리소스에 대한 프라이빗 인증서를 생성하고 인증서 수명 주기를 중앙에서 관리할 수 있습니다. ACM 통합 서비스와 함께 사용하기 AWS Certificate Manager 위해를 통해 프로비저닝된 퍼블릭 및 프라이빗 인증서는 무료입니다. 애플리케이션을 실행하기 위해 생성한 AWS 리소스에 대해서만 비용을 지불합니다. 를 사용하면의 작업 AWS Private CA 과 발급한 프라이빗 인증서에 대해 매월 [AWS Private Certificate Authority](#)요금을 지불합니다. 자세한 내용은 [AWS Certificate Manager - AWS 문서를 참조하세요](#).

AWS Managed Services FAQ의 ACM

일반적인 질문과 답변:

Q: AMS 계정 AWS Certificate Manager 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)
를 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다
customer_acm_create_role. 이 역할을 사용하여 ACM 인증서를 생성하고 관리할 수 있습니다.
계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

customer_acm_create_role IAM 역할을 추가하지 않은 경우에도 다음 변경 유형을 사용하여 ACM 인증서를 생성할 수 있습니다.

- [ACM | 퍼블릭 인증서 생성](#)
- [ACM | 프라이빗 인증서 생성](#)
- [추가 SANs 포함된 ACM 인증서 | 생성](#)

Q: 사용에 대한 제한 사항은 무엇입니까 AWS Certificate Manager?

기존 인증서를 삭제하거나 수정하려면 변경 요청(RFC)을 AMS에 제출해야 합니다. 이러한 작업을 수행하려면 전체 관리자 액세스 권한이 필요합니다(관리 | 기타 | 기타 | 변경 유형 업데이트 (ct-0xdawir96cy7k)). IAM 정책은 태그 이름(mc*, ams* 등)을 기반으로 권한을 제외할 수 없습니다. 인증서에는 비용이 발생하지 않으므로 사용하지 않는 인증서를 삭제하는 것은 시간에 민감하지 않습니다.

Q: Certificate Manager를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

기존 퍼블릭 DNS 이름 및 DNS CNAME 레코드를 생성하기 위한 액세스 권한은 관리형 계정에서 호스팅할 필요가 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Private Certificate Authority 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AWS Private Certificate Authority 기능에 직접 액세스할 수 있습니다. 프라이빗 인증서는 프라이빗 네트워크에서 연결된 리소스 간의 통신을 식별하고 보호하는 데 사용됩니다. 서버, 모바일, 및 IoT 디바이스 및 애플리케이션. AWS Private CA 는 프라이빗 인증서의 수명 주기를 쉽고 안전하게 관리하는 데 도움이 되는 관리형 프라이빗 CA 서비스입니다.는 자체 프라이빗 CA 운영에 대한 선결제 투자 및 지속적인 유지 관리 비용 없이 가용성이 높은 프라이빗 CA 서비스를 AWS Private CA 제공합니다.는 ACM의 인증서 관리 기능을 프라이빗 인증서로 AWS Private CA 확장합니다. 를 사용하면 퍼블릭 및 프라이빗 인증서를 중앙에서 생성하고 관리할 수 있습니다. AWS Management Console 또는 ACM API를 사용하여 AWS 리소스에 대한 프라이빗 인증서를 쉽게 생성하고 배포할 수 있습니다. EC2 인스턴스, 컨테이너, IoT 디바이스 및 온프레미스 리소스의 경우 프라이빗 인증서를 쉽게 생성 및 추적하고 자체 클라이언트 측 자동화 코드를 사용하여 배포할 수 있습니다. 또한 사용자 지정 인증서 수명, 키 알고리즘 또는 리소스 이름이 필요한 애플리케이션에 대해 프라이빗 인증서를 생성하고 직접 관리할 수 있는 유연성도 있습니다. 자세한 내용은 섹션을 참조하세요 [AWS Private CA](#).

AWS Private CA AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Private CA 에서 액세스를 요청하려면 어떻게 해야 하나요?

AWS 서비스 RFC(관리 | AWS 서비스 | 호환 서비스) 제출을 통해 액세스를 요청합니다. 이 RFC를 통해 계정에 다음 IAM 역할이 프로비저닝됩니다. `customer_acm_pca_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS Private CA?

현재 AWS Resource Access Manager (AWS RAM)는 교차 계정을 공유하는 데 사용할 수 있는 AWS Private CA 없습니다.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS Private CA?

1. CRL을 생성하려는 경우 저장할 S3 버킷이 필요합니다. AWS Private CA는 지정된 Amazon S3 버킷에 CRL을 자동으로 저장하고 주기적으로 업데이트합니다. CRL을 설정하려면 먼저 S3 버킷에 아래 버킷 정책이 있어야 합니다. 이 요청을 진행하려면 다음과 같이 `ct-0fpjlx808sh2`(관리 | 고급 스택 구성 요소 | S3 스토리지 | 정책 업데이트)를 사용하여 RFC를 생성합니다.

- S3 버킷 이름 또는 ARN을 입력합니다.
- 아래 정책을 RFC에 복사하고 원하는 S3 버킷 이름으로 `bucket-name` 바꿉니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "acm-pca.amazonaws.com"
      },
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*",
        "arn:aws:s3:::bucket-name"
      ]
    }
  ]
}
```

```
]
}
```

2. 위의 S3 버킷이 암호화된 경우 서비스 보안 주체 `acm-pca.amazonaws.com` 복호화 권한이 필요합니다. 이 요청을 진행하려면 다음과 같이 `ct-3ovo7px2vsa6n`(관리 | 고급 스택 구성 요소 | KMS 키 | 업데이트)을 사용하여 RFC를 생성합니다.

- 정책을 업데이트해야 하는 KMS 키 ARN을 제공합니다.
- 아래 정책을 RFC에 복사하고를 원하는 S3 버킷 이름으로 `bucket-name` 바꿉니다.

```
{
  "Sid": "Allow ACM-PCA use of the key",
  "Effect": "Allow",
  "Principal": {
    "Service": "acm-pca.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": [
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
        "arn:aws:s3:::bucket_name/audit-report/*",
        "arn:aws:s3:::bucket_name/crl/*"
      ]
    }
  }
}
```

3. AWS Private CA CRLs S3 설정 "새 ACLs)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단"을 지원하지 않습니다. 가 ACM Private CA용 CRLs을 안전하게 생성 및 저장하는 방법에 설명된 대로 CRL을 AWS Private CA 작성하도록 허용하려면 S3 계정 및 버킷에서이 설정을 비활성화해야 합니다. 비활성화하려면 `ct-0xdawir96cy7k`(관리 | 기타 | 기타 | 업데이트)를 사용하여 새 RFC를 생성하고 위험 수락을 연결합니다. <https://aws.amazon.com/blogs/security/how-to-securely-create-and-store-your-crl-for-acm-private-ca/> 위험 수락에 대한 질문이 있는 경우 Cloud Architect에 문의하세요.

AMS SSP를 사용하여 AMS 계정에서 AWS CloudEndure 프로비저닝

Note

가 성공적으로 출시되면 이제 모든 AWS 리전에서 AWS Application Migration Service CloudEndure 마이그레이션 서비스의 수명이 종료됩니다. GovCloud 리전 및 상용 리전으로 AWS Application Migration Service 의 리프트 앤 시프트 마이그레이션에는를 사용하는 것이 좋습니다. 자세한 내용은 [란 무엇입니까 AWS Application Migration Service?](#)를 참조하세요. 를 사용하려면 CA에 AWS Application Migration Service문의하여 안내를 받으세요.

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS CloudEndure 기능에 액세스합니다. AWS CloudEndure 마이그레이션은 물리적, 가상 및 클라우드 기반 인프라에서 대규모 마이그레이션을 간소화, 가속화 및 자동화합니다 AWS. CloudEndure 재해 복구(DR)는 랜섬웨어 및 서버 손상을 포함한 모든 위협으로부터 가동 중지 시간과 데이터 손실을 방지합니다.

AWS Managed Services FAQ의AWS CloudEndure

Q: AMS 계정에서 CloudEndure에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 사용자를 프로비저닝합니다customer_cloud_endure_user. 계정에 프로비저닝되면 사용자의 액세스 키와 보안 키가 AWS Secrets Manager에서 공유됩니다.

이러한 정책은 및 계정도 프로비저닝됩니다

다customer_cloud_endure_policycustomer_cloud_endure_deny_policy.

또한 애플리케이션 통합을 위한 CloudEndure DR 솔루션에는 인프라 변경 권한이 있으므로 위협 수락을 제공해야 합니다. 이렇게 하려면 클라우드 서비스 제공 관리자(CSDM)와 협력하세요.

Q: AMS 계정에서 CloudEndure를 사용하는 데 따르는 제한 사항은 무엇인가요?

Cloud Endure 복제 및 변환 인스턴스는 지정된 서브넷에서만 시작할 수 있습니다.

Q: AMS 계정에서 CloudEndure를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요? RFC 양방향 서신을 통해 다음을 공유합니다.

- 시작할 복제 및 변환 인스턴스에 대한 VPC 서브넷 세부 정보입니다.
- EBS 볼륨이 암호화된 경우 KMS 키 Amazon 리소스 이름(ARN)입니다.

AMS SSP를 사용하여 AMS 계정 AWS CloudHSM 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AWS CloudHSM 기능에 직접 액세스할 AWS CloudHSM 수 있습니다. 기업, 계약, 및 AWS 클라우드 내에서 전용 하드웨어 보안 모듈(HSM) 인스턴스를 사용하여 데이터 보안을 위한 규정 준수 요구 사항을 충족합니다. AWS 및 AWS Marketplace 파트너, 는 AWS 플랫폼 내에서 민감한 데이터를 보호하기 위한 다양한 솔루션을 제공합니다. 그러나 암호화 키 관리를 위한 계약 또는 규제 명령이 적용되는 일부 애플리케이션 및 데이터의 경우 추가 보호가 필요할 수 있습니다.는 기존 데이터 보호 솔루션을 AWS CloudHSM 보완하고 보안 키 관리를 위해 정부 표준에 따라 설계되고 검증된 HSMs 내에서 암호화 키를 보호할 수 있습니다.를 AWS CloudHSM 사용하면 안전하게 생성하고, 스토어, 및는 사용자만 키에 액세스할 수 있는 방식으로 데이터 암호화에 사용되는 암호화 키를 관리합니다. 자세한 내용은 [AWS CloudHSM](#)를 참조하세요.

AWS CloudHSM AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS CloudHSM 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AMS 계정에서를 사용하는 것은 2단계 프로세스입니다.

1. AWS CloudHSM 클러스터를 요청합니다. 관리 | 기타 | 기타 | 생성(ct-1e1xtak34nx76) 변경 유형을 사용하여 RFC를 제출하여이 작업을 수행합니다. 다음 세부 정보를 포함합니다.
 - AWS 리전.
 - VPC ID/ARN. 제출하는 RFC와 동일한 계정에 있는 VPC ID/VPC ARN을 제공합니다.
 - 클러스터에 대해 두 개 이상의 가용 영역을 지정합니다.
 - HSM 클러스터에 연결할 Amazon EC2 인스턴스 ID입니다.
2. AWS CloudHSM 콘솔에 액세스합니다. 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가 (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여이 작업을 수행합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_cloudhsm_console_role.

계정에 역할이 프로비저닝된 후 페더레이션 솔루션에 온보딩해야 합니다.

Q: AMS 계정 AWS CloudHSM 에서 사용에 대한 제한 사항은 무엇인가요?

AWS CloudHSM 콘솔에 대한 액세스는 클러스터를 생성, 종료 또는 복원할 수 있는 기능을 제공하지 않습니다. 이러한 작업을 수행하려면 관리 | 기타 | 기타 | 변경 유형 생성(ct-1e1xtak34nx76) 변경 유형을 제출합니다.

Q: AMS 계정 AWS CloudHSM 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

VPC 내의 클라이언트 Amazon EC2 인스턴스를 통해 포트 2225를 사용하는 TCP 트래픽을 허용하거나 HSM 클러스터에 액세스하려는 온프레미스 서버에 Direct Connect VPN을 사용해야 합니다. AWS CloudHSM 는 보안 그룹 및 네트워크 인터페이스에 Amazon EC2를 사용합니다. 로그 모니터링 또는 감사를 위해 HSM은 모든 로컬 HSM 디바이스 활동에 CloudTrail(AWS API 작업) 및 CloudWatch Logs를 사용합니다.

Q: AWS CloudHSM 클라이언트 및 관련 소프트웨어 라이브러리에 업데이트를 적용하는 사람은 누구입니까?

라이브러리 및 클라이언트 업데이트를 적용할 책임은 사용자에게 있습니다. [CloudHSM 버전 기록](#) 페이지에서 릴리스를 모니터링한 다음 [CloudHSM 클라이언트 업그레이드](#)를 사용하여 업데이트를 적용해야 합니다.

 Note

HSM 어플라이언스용 소프트웨어 패치는 항상 서비스에서 AWS CloudHSM 자동으로 적용됩니다.

AMS SSP를 사용하여 AMS 계정 AWS CodeBuild 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS CodeBuild 기능에 액세스할 수 있습니다. AWS CodeBuild 는 소스 코드를 컴파일하고, 테스트를 실행하고, 배포할 준비가 된 소프트웨어 패키지를 생성하는 완전 관리형 지속적 통합 서비스입니다. CodeBuild를 사용하면 자체 빌드 서버를 프로비저닝, 관리 및 조정할 필요가 없습니다. CodeBuild는 지속적으로 규모가 조정되며 여러 빌드를 동시에 처리하기 때문에 빌드가 대기열에서 대기하지 않고 바로 처리됩니다. 사전 패키징된 빌드 환경을 사용하면 신속하게 시작할 수 있으며 혹은 자체 빌드 도구를 사용하는 사용자 지정 빌드 환경을 만들 수 있습니다. CodeBuild를 사용하면 컴퓨팅 리소스에 대한 분당 사용 요금이 청구됩니다. 자세한 내용은 [AWS CodeBuild](#)를 참조하세요.

 Note

단일 RFC로 CodeCommit, CodeBuild, CodeDeploy 및 CodePipeline을 온보딩하려면 Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 변경 유형을 제출하고 CodeBuild, CodeDeploy 및 CodePipeline의 세 가지 서비스를 요청합니다. 그런 다음 ,

customer_codebuild_service_role customer_codedeploy_service_role 및 세 가지 역할 aws_code_pipeline_service_role 이 모두 계정에 프로비저닝됩니다. 계정에 프로비저닝한 후 페더레이션 솔루션의 역할을 온보딩해야 합니다.

AWS Managed Services FAQ의 CodeBuild

일반적인 질문과 답변:

Q: AMS 계정 AWS CodeBuild 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AMS 계정 AWS CodeBuild 에서를 사용하는 과정은 2단계로 이루어집니다.

1. S3 버킷, Amazon CloudWatch 및 로그 그룹과 AWS 조정하도록 빌드 프로세스를 CodeBuild Service Role 위한 프로비저닝
2. CodeBuild 콘솔에 대한 액세스 요청

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 AMS 계정에 둘 다 설정하도록 요청할 수 있습니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS CodeBuild 에서 사용에 대한 제한 사항은 무엇인가요?

AWS CodeBuild 콘솔 관리자 액세스의 경우 리소스 수준에서 권한이 제한됩니다. 예를 들어 CloudWatch 작업은 특정 리소스로 제한되고 iam:PassRole 권한은 제어됩니다.

Q: AMS 계정에서 CodeBuild를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

정의된 AWS CodeBuild 서비스 역할에 추가 IAM 권한이 필요한 경우 AMS 서비스 요청을 통해 요청합니다.

AMS SSP를 사용하여 AMS 계정 AWS CodeCommit 에서 프로비저닝

Note

AWS 는 2024년 7월 25 AWS CodeCommit 일부부터 새로운 고객 액세스를 종료했습니다. AWS CodeCommit 기존 고객은 서비스를 정상적으로 계속 사용할 수 있습니다. AWS 는에 대한 보안, 가용성 및 성능 개선에 계속 투자 AWS CodeCommit 하지만 새로운 기능을 도입할 계획은 없습니다.

AWS CodeCommit Git 리포지토리를 다른 Git 공급자로 마이그레이션하려면 클라우드 아키텍트(CA)에 문의하여 지침을 받으세요. Git 리포지토리 마이그레이션에 대한 자세한 내용은 [AWS CodeCommit 리포지토리를 다른 Git 공급자로 마이그레이션하는 방법을 참조하세요](#).

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS CodeCommit 기능에 액세스할 수 있습니다. AWS CodeCommit 는 보안 Git 기반 리포지토리를 호스팅하는 완전 관리형 [소스 제어](#) 서비스입니다. 이를 통해 팀은 안전하고 확장성이 뛰어난 에코시스템에서 코드에 대해 협업할 수 있습니다. CodeCommit을 사용하면 자체 소스 제어 시스템을 운영하거나 인프라 규모 조정에 대해 걱정할 필요가 없습니다. CodeCommit을 사용하여 소스 코드에서 바이너리에 이르기까지 모든 것을 안전하게 저장할 수 있으며 기존 Git 도구와 원활하게 작동합니다. 자세한 내용은 [AWS CodeCommit](#)를 참조하세요.

Note

CodeCommit, CodeBuild, CodeDeploy 및 CodePipeline을 단일 RFC로 온보딩하려면 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하고 CodeBuild, CodeDeploy 및 CodePipeline의 세 가지 서비스를 요청합니다. 그런 다음, customer_codebuild_service_role customer_codedeploy_service_role 및 세 가지 역할 aws_code_pipeline_service_role이 모두 계정에 프로비저닝됩니다. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

AWS Managed Services FAQ의 CodeCommit

Q: AMS 계정에서 CodeCommit에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AWS CodeCommit 콘솔 및 데이터 액세스 역할은 두 개의 AWS 서비스 RFCs

- Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 AWS CodeCommit 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_codecommit_console_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

데이터 액세스(예: 훈련 및 개체 목록)에는 S3 데이터 소스(필수), 출력 버킷(필수) 및 KMS(선택 사항)를 지정하는 각 데이터 소스에 대해 별도의 CTs가 필요합니다. 모든 데이터 소스에 액세스 역할이 부여된 한 AWS CodeCommit 작업 생성에는 제한이 없습니다. 데이터 액세스를 요청하려면 관리 | 기타 | 기타 | 생성(ct-1e1xtak34nx76)을 사용하여 RFC를 제출합니다.

Q: AMS 계정 AWS CodeCommit 에서 사용에 대한 제한 사항은 무엇입니까?

CodeCommit의 트리거 기능은 SNS 주제를 생성할 수 있는 관련 권한으로 인해 비활성화됩니다. CodeCommit에 대한 직접 인증은 제한되므로 사용자는 자격 증명 헬퍼로 인증해야 합니다. kms:Encrypt, , kms:Decrypt, kms:ReEncrypt, kms:GenerateDataKey, kms:GenerateDataKeyWithoutPlaintext등의 일부 KMS 명령도 제한됩니다. kms:DescribeKey.

Q: AMS 계정 AWS CodeCommit 에서 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

S3 버킷이 KMS 키로 암호화된 경우를 사용하려면 S3 및 KMS가 필요합니다 AWS CodeCommit.

AMS SSP를 사용하여 AMS 계정 AWS CodeDeploy 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS CodeDeploy 기능에 액세스할 수 있습니다. AWS CodeDeploy 는 Amazon EC2 AWS Fargate AWS Lambda 및 온프레미스 서버와 같은 다양한 컴퓨팅 서비스에 대한 소프트웨어 배포를 자동화하는 완전 관리형 배포 서비스입니다. AWS CodeDeploy 는 새 기능을 신속하게 릴리스하고, 애플리케이션 배포 중 가동 중지 시간을 방지하고, 애플리케이션 업데이트의 복잡성을 처리할 수 있도록 지원합니다. AWS CodeDeploy 를 사용하여 소프트웨어 배포를 자동화할 수 있으므로 오류가 발생하기 쉬운 수동 작업이 필요하지 않습니다. 서비스는 배포 요구 사항에 맞게 확장됩니다. 자세한 내용은 [AWS CodeDeploy](#)를 참조하세요.

Note

CodeCommit, CodeBuild, CodeDeploy 및 CodePipeline을 단일 RFC로 온보딩하려면 Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 변경 유형을 제출하고 CodeBuild, CodeDeploy 및 CodePipeline의 세 가지 서비스를 요청합니다. 그런 다음 , customer_codebuild_service_role customer_codedeploy_service_role 및 세 가지 역할 aws_code_pipeline_service_role이 모두 계정에 프로비저닝됩니다. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

AWS Managed Services FAQ의 CodeDeploy

Q: AMS 계정에서 CodeDeploy에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 CodeDeploy에 대한 액세스를 요청합니다. 이 RFC는 계정에 IAM 역할을 프로비저닝합니다. customer_codedeploy_console_role customer_codedeploy_service_role. 계정에

프로비저닝된 후에는 페더레이션 솔루션의 `customer_codedeploy_console_role` 역할을 온보딩해야 합니다.

Q: AMS 계정에서 CodeDeploy를 사용할 때 제한 사항은 무엇인가요?

현재 컴퓨팅 플랫폼은 Amazon EC2/온프레미스로만 지원됩니다. 블루/그린 배포는 지원되지 않습니다.

Q: AMS 계정에서 CodeDeploy를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 CodeDeploy를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS CodePipeline 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS CodePipeline 기능에 액세스할 수 있습니다. AWS CodePipeline 는 빠르고 안정적인 애플리케이션 및 인프라 업데이트를 위해 릴리스 파이프라인을 자동화하는 데 도움이 되는 완전 관리형 [지속적 전송](#) 서비스입니다. CodePipeline은 정의한 릴리스 모델을 기반으로 코드 변경이 있을 때마다 릴리스 프로세스의 구축, 테스트 및 배포 단계를 자동화합니다. 이를 통해 기능과 업데이트를 신속하고 안정적으로 제공할 수 있습니다. GitHub AWS CodePipeline 와 같은 타사 서비스 또는 자체 사용자 지정 플러그인과 쉽게 통합할 수 있습니다. AWS CodePipeline에서는 사용한 만큼만 비용을 지불합니다. 선수금이나 장기 약정을 적용하지 않습니다. 자세한 내용은 [AWS CodePipeline](#)를 참조하세요.

Note

단일 RFC로 CodeCommit, CodeBuild, CodeDeploy 및 CodePipeline을 온보딩하려면 Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 변경 유형을 제출하고 CodeBuild, CodeDeploy 및 CodePipeline의 세 가지 서비스를 요청합니다. 그런 다음, `customer_codebuild_service_role` `customer_codedeploy_service_role` 및 세 가지 역할 `aws_code_pipeline_service_role`이 모두 계정에 프로비저닝됩니다. 계정에 프로비저닝한 후 페더레이션 솔루션의 역할을 온보딩해야 합니다. AMS의 CodePipeline은 최소 권한 모델 및 AMS 변경 관리 프로세스를 우회하는 서비스 역할 및 정책을 생성하기 위해 승격된 권한이 필요하기 때문에 소스 단계에 대해 "Amazon CloudWatch Events"를 지원하지 않습니다.

AWS Managed Services FAQ의 CodePipeline

Q: AMS 계정에서 CodePipeline에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관련 계정 `customer_code_pipeline_console_role`에서에 대한 서비스 요청을 제출하여 CodePipeline에 대한 액세스를 요청합니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

현재 AMS Operations는 계정에 이 서비스 역할인 `aws_code_pipeline_service_role_policy`도 배포합니다.

Q: AMS 계정에서 CodePipeline을 사용할 때 제한 사항은 무엇인가요?

예. CodePipeline 기능, 단계 및 공급자는 다음으로 제한됩니다.

1. 배포 단계: Amazon S3로 제한 및 AWS CodeDeploy
2. 소스 단계: Amazon S3, AWS CodeCommit, BitBucket 및 GitHub로 제한됨
3. 빌드 단계: AWS CodeBuild 및 Jenkins로 제한됨
4. 승인 단계: Amazon SNS로 제한됨
5. 테스트 단계: 제한 대상 AWS CodeBuild, Jenkins, BlazeMeter, Ghost Inspector UI Testing, Micro Focus StormRunner Load 및 Runscope API Monitoring
6. 호출 단계: Step Functions 및 Lambda로 제한

Note

AMS 작업은 `customer_code_pipeline_lambda_policy` 계정에 배포되며 Lambda 간접 호출 단계에 대한 Lambda 실행 역할에 연결되어야 합니다. 이 정책을 추가할 Lambda 서비스/실행 역할 이름을 제공하세요. 사용자 지정 Lambda 서비스/실행 역할이 없는 경우 AMS는 라는 새 역할을 생성합니다. `customer_code_pipeline_lambda_execution_role`이 역할은와 `customer_lambda_basic_execution_role` 함께의 사본이 됩니다 `customer_code_pipeline_lambda_policy`.

Q: AMS 계정에서 CodePipeline을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AWS 지원되는 서비스는 CodePipeline 시작 전 또는 이와 함께 시작해야 AWS CodeCommit AWS CodeBuild AWS CodeDeploy 합니다.

AMS SSP를 사용하여 AMS 계정 AWS Compute Optimizer 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Compute Optimizer 기능에 액세스할 수 있습니다. AWS Compute Optimizer 는 기계 학습을 사용하여 과거 사용

를 지표를 분석하여 비용을 절감하고 성능을 개선하기 위해 워크로드에 최적의 AWS 컴퓨팅 리소스를 권장합니다. 컴퓨팅(Amazon EC2 및 ASGs)을 과도하게 프로비저닝하면 불필요한 인프라 비용이 발생하고 컴퓨팅을 과소 프로비저닝하면 애플리케이션 성능이 저하될 수 있습니다. Compute Optimizer를 사용하면 사용률 데이터를 기반으로 Amazon EC2 Auto Scaling 그룹에 속하는 인스턴스 유형을 포함하여 최적의 Amazon EC2 인스턴스 유형을 선택할 수 있습니다. 자세한 내용은 [AWS Compute Optimizer](#)를 참조하세요.

AWS Managed Services FAQ의 Compute Optimizer

Q: AMS 계정에서 Compute Optimizer에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_compute_optimizer_readonly_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Compute Optimizer를 사용할 때 제한 사항은 무엇인가요?

제한은 없습니다. 의 전체 기능은 AMS 계정에서 AWS Compute Optimizer 사용할 수 있습니다.

Q: AMS 계정에서 Compute Optimizer를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- 계정에서 서비스를 활성화하려면 AMS Ops에 권한을 부여하는 RFC(관리 | 기타 | 기타 | 업데이트)를 제출해야 합니다. 배포 중에 지표 수집 및 보고서 생성을 허용하는 서비스 연결 역할(SLR)이 생성됩니다. SLR에는 “AWSServiceRoleForComputeOptimizer” 레이블이 지정되어 있습니다. 자세한 내용은 [에 대한 서비스 연결 역할 사용을 참조하세요. AWS Compute Optimizer](#)
- 다음 지표에 대해 CloudWatch 지표를 활성화해야 합니다.
 - CPU 사용률: 인스턴스에서 사용 중인 할당된 Amazon EC2 컴퓨팅 유닛의 백분율입니다. 이 지표는 선택한 인스턴스에서 애플리케이션을 실행하는 데 필요한 처리 능력을 식별합니다.
 - 메모리 사용률: 샘플 기간 동안 어떤 식으로든 사용된 메모리의 양입니다. 이 지표는 선택한 인스턴스에서 애플리케이션을 실행하는 데 필요한 메모리를 식별합니다. 메모리 사용률은 통합된 CloudWatch 에이전트가 설치된 리소스에 대해서만 분석됩니다. 자세한 내용은 CloudWatch 에이전트를 사용하여 메모리 사용률 활성화(10페이지)를 참조하세요.
 - 네트워크 입력: 인스턴스가 모든 네트워크 인터페이스에서 수신한 바이트 수입니다. 이 지표는 단일 인스턴스로 들어오는 네트워크 트래픽의 볼륨을 식별합니다.
 - 네트워크 출력: 인스턴스가 모든 네트워크 인터페이스에서 보낸 바이트 수입니다. 이 지표는 단일 인스턴스에서 나가는 네트워크 트래픽의 양을 식별합니다.

- 로컬 디스크 입력/출력(I/O): 로컬 디스크의 입력/출력 작업 수입니다. 이 지표는 인스턴스의 루트 볼륨 성능을 식별합니다.

AMS SSP를 사용하여 AMS 계정 AWS DataSync 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS DataSync 기능에 액세스할 수 있습니다. 온프레미스 스토리지와 Amazon S3, Amazon Elastic File System(Amazon Elastic File System) 또는 Amazon FSx 간에 대량의 데이터를 온라인으로 AWS DataSync 이동합니다. 데이터 전송과 관련된 수동 작업은 마이그레이션 속도를 늦추고 IT 운영에 부담을 줄 수 있습니다. DataSync는 복사 작업 스크립팅, 전송 예약 및 모니터링, 데이터 검증, 네트워크 사용을 최적화 등 이러한 많은 작업을 제거하거나 자동으로 처리합니다. DataSync 소프트웨어 에이전트는 NFS(Network File System) 및 SMB(Server Message Block) 스토리지에 연결되므로 애플리케이션을 수정할 필요가 없습니다. DataSync는 인터넷 또는 AWS Direct Connect 링크를 통해 오픈 소스 도구보다 최대 10배 빠른 속도로 수백 테라바이트와 수백만 개의 파일을 전송할 수 있습니다. DataSync를 사용하여 활성 데이터 세트 또는 아카이브를 로 마이그레이션하거나 AWS, 시기 적절한 분석 및 처리를 위해 클라우드로 데이터를 전송하거나, 비즈니스 연속성 AWS 을 위해 데이터를 복제할 수 있습니다.

자세한 내용은 [AWS DataSync](#)를 참조하세요.

AWS Managed Services의 DataSync FAQ

Q: AMS 계정에서 DataSync에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_datsync_console_role.

계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

작업 로그를 스트리밍하는 데 사용할 CloudWatch 로그 그룹은 "/aws/datsync"입니다.

Q: AMS 계정에서 DataSync를 사용할 때 제한 사항은 무엇인가요?

의 전체 기능은 AMS 계정에서 AWS DataSync 사용할 수 있습니다.

Q: AMS 계정에서 DataSync를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- DataSync 서비스 역할을 사용하여 수행할 DataSync 작업과 연결된 모든 S3 버킷에는 Amazon S3 ARNs(Amazon 리소스 이름)이 필요합니다customer_datsync_service_role. DataSync

- DataSync 에이전트의 VPC 엔드포인트 및 보안 그룹은 VPC 엔드포인트를 사용하기 전에 관리 | 기타 | 기타 | 생성(ct-1e1xtak34nx76) 변경 유형이 있는 RFC로 요청해야 합니다.
- AWS DataSync 에이전트는 AMS에서 어플라이언스로 실행됩니다. AWS DataSync 에이전트는 서비스에 의해 패치되고 업데이트됩니다. 자세한 내용은 [AWS DataSync FAQ](#)를 참조하세요.
- AWS DataSync 에이전트를 시작하려면 관리 | 기타 | 기타 | 생성(ct-1e1xtak34nx76) 변경 유형을 사용하여 RFC를 제출하여 에이전트 배포를 요청합니다. AWS DataSync Amazon EC2 AMI ID, 인스턴스 유형, 서브넷, 보안 그룹을 제공하고 기존 Amazon EC2 키 페어를 참조하거나 새 키 페어 생성을 요청합니다.

Note

AMS는 고객을 대신하여 AWS DataSync 에이전트를 수동으로 프로비저닝하며 AWS DataSync Amazon EC2 AMI에서 WIGS 수집 프로세스가 필요하지 않습니다.

AMS SSP를 사용하여 AMS 계정 AWS Device Farm 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS Device Farm 기능에 액세스할 수 있습니다. AWS Device Farm 는 테스트 인프라를 프로비저닝하고 관리할 필요 없이 광범위한 데스크톱 브라우저 및 실제 모바일 디바이스에서 웹 및 모바일 앱을 테스트하여 웹 및 모바일 앱의 품질을 개선할 수 있는 애플리케이션 테스트 서비스입니다. 이 서비스를 사용하면 여러 데스크톱 브라우저 또는 실제 디바이스에서 동시에 테스트를 실행하여 테스트 제품군 실행 속도를 높이고 비디오와 로그를 생성하여 앱 문제를 빠르게 식별할 수 있습니다.

자세한 내용은 [AWS Device Farm](#)를 참조하세요.

AWS Device Farm AWS Managed Services FAQ의

Q: AMS 계정 AWS Device Farm 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_devicefarm_role.

계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Device Farm 에서 사용에 대한 제한 사항은 무엇인가요?

'Name' 태그에서 AMS 네임스페이스를 사용하는 경우를 제외하고 AWS Device Farm 서비스에 대한 전체 액세스 권한이 제공됩니다.

Q: AMS 계정 AWS Device Farm 에서 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

없음.

AMS SSP를 사용하여 AMS 계정 AWS Elastic Disaster Recovery 에서 프로 비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS Elastic Disaster Recovery 기능에 액세스할 수 있습니다.는 저렴한 스토리지, 최소 컴퓨팅 및 point-in-time으 로 복구를 사용하여 온프레미스 및 클라우드 기반 애플리케이션을 빠르고 안정적으로 복구하여 가 동 중지 시간과 데이터 손실을 AWS Elastic Disaster Recovery 최소화합니다. AWS Elastic Disaster Recovery 를 사용하여 지원되는 운영 체제에서 실행되는 온프레미스 또는 클라우드 기반 애플리케이션을 복제할 때 IT 복원력을 높일 수 있습니다. AWS Management Console 를 사용하여 복제 및 시작 설정을 구성하고, 데이터 복제를 모니터링하고, 드릴 또는 복구를 위해 인스턴스를 시작합니다.

자세한 내용은 [AWS Elastic Disaster Recovery](#)를 참조하세요.

AWS Elastic Disaster Recovery AWS Managed Services FAQ의

Q: AMS 계정 AWS Elastic Disaster Recovery 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유 형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니 다customer_drs_console_role.

계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Elastic Disaster Recovery 에서 사용에 대한 제한 사항은 무엇인가요?

AMS 계정 AWS Elastic Disaster Recovery 에서 사용할 수 있는 제한은 없습니다.

Q: AMS 계정 AWS Elastic Disaster Recovery 에서 사용하기 위한 사전 조건 또는 종속성은 무엇입 니까?

- 콘솔 역할에 액세스한 후에는 Elastic Disaster Recovery 서비스를 초기화하여 계정 내에서 필요한 IAM 역할을 생성해야 합니다.
- 인스턴스 프로파일의 복제본을 생성하고
AWSElasticDisasterRecoveryEc2InstancePolicy 정책을 customer-mc-ec2-
instance-profile 연결하려면 변경 유형 관리 | 애플리케이션 | IAM 인스턴스 프로파일 | 변경

유형 생성(검토 필요) ct-0ixp4ch2tiu04 RFC를 제출해야 합니다. 새 정책을 연결할 시스템을 지정해야 합니다.

- 인스턴스가 기본 인스턴스 프로파일을 사용하지 않는 경우 AMS는 자동화를 AWSElasticDisasterRecoveryEc2InstancePolicy 통해 연결할 수 있습니다.
- 교차 계정 복구에는 고객 소유 KMS 키를 사용해야 합니다. 대상 계정 액세스를 허용하려면 정책에 따라 소스 계정의 KMS 키를 업데이트해야 합니다. 자세한 내용은 [대상 계정과 EBS 암호화 키 공유를 참조하세요](#).
- 볼 역할을 전환하지 않으려면 허용에서 정책을 customer_drs_console_role 볼 수 있도록 KMS 키 정책을 업데이트해야 합니다.
- 교차 계정, 교차 리전 재해 복구의 경우 AMS는 소스 및 대상 계정을 신뢰할 수 있는 계정으로 설정하고 [장애 복구 및 AWS 오른쪽 크기 조정 역할을](#) 통해 배포해야 합니다 AWS CloudFormation.

AMS SSP를 사용하여 AMS 계정 AWS Elemental MediaConvert 에서 프로 비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Elemental MediaConvert 기능에 액세스할 수 있습니다. AWS Elemental MediaConvert 는 브로드캐스트 등급 기능이 있는 파일 기반 비디오 트랜스코딩 서비스입니다. 이를 통해 대규모로 브로드캐스트 및 멀티스크린 전송을 위한 video-on-demand(VOD) 콘텐츠를 생성할 수 있습니다. 이 서비스는 고급 비디오 및 오디오 기능을 간단한 웹 서비스 인터페이스 및 pay-as-you-go 요금과 결합합니다. 를 사용하면 자체 비디오 처리 인프라를 구축하고 운영하는 복잡성에 대해 걱정할 필요 없이 매력적인 미디어 경험을 제공하는 데 집중할 AWS Elemental MediaConvert 수 있습니다.

자세한 내용은 [AWS Elemental MediaConvert](#)를 참조하세요.

AWS Managed Services FAQ의 MediaConvert

Q: AMS 계정에서 MediaConvert에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_mediaconvert_author_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

소스 S3 버킷에서 읽고 대상 S3 버킷에 출력을 쓰S3고 디지털 권한 관리(DRM)customer_MediaConvert_Default_Role가 필요한 경우 API 게이트웨이를 호출하기 위해 MediaConvert에서 사용하는 두 번째 역할인이 제공됩니다.

Q: AMS 계정에서 MediaConvert를 사용할 때 적용되는 제한 사항은 무엇인가요?

AMS에서 MediaConvert를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 MediaConvert를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정에서 MediaConvert를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Elemental MediaLive 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Elemental MediaLive 기능에 액세스할 수 있습니다. AWS Elemental MediaLive 는 브로드캐스트급 라이브 비디오 처리 서비스입니다. 이를 통해 TV 방송 및 연결된 TV, 태블릿, 스마트폰, 셋톱 박스와 같은 인터넷 연결 멀티스크린 디바이스로 전송하기 위한 고품질 비디오 스트림을 생성할 수 있습니다. 이 서비스는 실시간 비디오 스트림을 인코딩하고, 더 큰 크기의 라이브 비디오 소스를 가져와 뷰어에게 배포할 수 있도록 더 작은 버전으로 압축하는 방식으로 작동합니다. AWS Elemental MediaLive를 사용하면 고급 방송 기능, 고가용성 및 pay-as-you-go 요금을 사용하여 라이브 이벤트와 24x7 채널 모두에 대한 스트림을 쉽게 설정할 수 있습니다. AWS Elemental MediaLive 를 사용하면 방송 등급 비디오 처리 인프라를 구축하고 운영하는 복잡성 없이 시청자에게 매력적인 라이브 비디오 경험을 만드는 데 집중할 수 있습니다.

자세한 내용은 [AWS Elemental MediaLive](#)를 참조하세요.

AWS Managed Services FAQ의 MediaLive

Q: AMS 계정에서 MediaLive에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다: `customer_medialive_author_role`.

이 RFC의 일부로 두 번째 역할이 계정에 배포됩니다. `customer_medialive_service_role` 역할은 Media Live 채널 및 입력에 할당되어 Amazon S3, MediaStore 및 CloudWatch Logs와 같은 다른 서비스와 상호 작용할 수 있습니다.

계정에 역할이 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 MediaLive를 사용할 때 제한 사항은 무엇인가요?

AMS에서 MediaLive를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 MediaLive를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정에서 MediaLive를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Elemental MediaPackage 에서 프로 비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Elemental MediaPackage 기능에 액세스할 수 있습니다.는 인터넷을 통한 전송을 위해 비디오를 AWS Elemental MediaPackage 안정적으로 준비하고 보호합니다. 단일 비디오 입력에서는 연결된 TVs, 컴퓨터, 태블릿 및 게임 콘솔에서 재생할 수 있는 형식의 비디오 스트림을 AWS Elemental MediaPackage 생성합니다. 이를 통해 DVRs에서 일반적으로 볼 수 있는 것과 같이 뷰어에게 인기 있는 비디오 기능(시작, 일시 중지, 되감기 등)을 쉽게 구현할 수 있습니다. AWS Elemental MediaPackage 는 디지털 권한 관리(DRM)를 사용하여 콘텐츠를 보호할 수도 있습니다.는 로드 에 따라 자동으로 AWS Elemental MediaPackage 규모를 조정하므로 뷰어는 필요한 용량을 미리 정확하게 예측하지 않고도 항상 훌륭한 경험을 할 수 있습니다.

자세한 내용은 [AWS Elemental MediaPackage](#)를 참조하세요.

AWS Managed Services MediaPackage FAQ

Q: AMS 계정 AWS Elemental MediaPackage 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_mediapackage_author_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

S3 및 Secrets Manager와 같은 다른 서비스와 상호 작용하기 위해 Media Live 채널 및 입력에 할당할 수 있는 두 번째 역할customer_mediapackage_service_role인이 제공됩니다.

Q: AMS 계정에서 MediaPackage를 사용할 때 제한 사항은 무엇인가요?

AMS에서 MediaPackage를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 MediaPackage를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

AMS 계정에서 MediaPackage를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Elemental MediaStore 에서 프로비저닝

Note

신중한 고려 후 AWS 는 2025년 11월 13일부터 MediaStore를 중단하기로 결정했습니다. MediaStore의 활성 고객인 경우 서비스 지원이 종료되는 2025년 11월 13일까지 MediaStore를 정상적으로 사용할 수 있습니다. 이 날짜 이후에는 MediaStore 또는 이 서비스에서 제공하는 기능을 더 이상 사용할 수 없습니다.

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Elemental MediaStore 기능에 액세스할 수 있습니다. AWS Elemental MediaStore 는 미디어에 최적화된 AWS 스토리지 서비스입니다. 라이브 스트리밍 비디오 content. AWS Elemental MediaStore acts를 비디오 워크플로의 오리진 스토어로 제공하는 데 필요한 성능, 일관성 및 짧은 지연 시간을 제공합니다. 고성능 기능은 장기적이고 비용 효율적인 스토리지와 함께 가장 까다로운 미디어 전송 워크로드의 요구 사항을 충족합니다. 자세한 내용은 [AWS Elemental MediaStore](#)를 참조하세요.

AWS Managed Services FAQ의 MediaStore

Q: AMS 계정에서 MediaStore에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 MediaStore에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_mediastore_author_role. 이 RFC의 일부로 두 번째 역할이 계정에 배포됩니다. 이 역할은 해당 기능을 활성화하도록 선택한 경우 MediaStore 서비스가 CloudWatch에서 활동을 로깅하는 데 사용하는 MediaStoreAccessLogs 역할입니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

현재 AMS Operations는 계정에이 서비스 역할인 도 배포합니다aws_code_pipeline_service_role_policy.

Q: AMS 계정에서 MediaStore를 사용할 때 제한 사항은 무엇인가요?

AMS에서 MediaStore를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 MediaStore를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정에서 MediaStore를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Elemental MediaTailor 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AWS Elemental MediaTailor 기능에 직접 액세스할 수 있습니다. AWS Elemental MediaTailor lets 비디오 공급자는 브로드캐스트 수준 quality-of-service 저하시키지 않고 비디오 스트림에 개별 대상 광고를 삽입합니다. 를 사용하면 라이브 또는 온디맨드 비디오의 AWS Elemental MediaTailor 시청자는 콘텐츠를 맞춤형 광고와 결합하는 스트림을 수신합니다. 그러나 다른 개인 맞춤형 광고 솔루션과 달리 AWS Elemental MediaTailor 전체 스트림, 즉 비디오 및 광고는 시청자의 경험을 개선하기 위해 브로드캐스트 등급 비디오 품질로 제공됩니다.는 클라이언트 및 서버 측 광고 전송 지표를 모두 기반으로 자동 보고를 AWS Elemental MediaTailor 제공하여 광고 노출 및 시청자 동작을 정확하게 측정합니다. 를 사용하면 선결제 비용 없이 예상치 못한 고수요 시청 이벤트를 쉽게 수익화할 수 있습니다 AWS Elemental MediaTailor. 또한 광고 전송률을 개선하여 모든 비디오에서 더 많은 비용을 절감할 수 있으며 다양한 콘텐츠 전송 네트워크, 광고 결정 서버 및 클라이언트 디바이스에서 작동합니다.

자세한 내용은 [AWS Elemental MediaTailor](#)를 참조하세요.

AWS Managed Services FAQ의 MediaTailor

Q: AMS 계정에서 MediaTailor에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC 를 제출하여 MediaTailor에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝 합니다customer-mediatailor-role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 MediaTailor를 사용할 때 제한 사항은 무엇인가요?

AMS에서 MediaTailor를 사용하는 데는 제한이 없습니다.

Q: AMS 계정에서 MediaTailor를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정에서 MediaTailor를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Global Accelerator 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 Global Accelerator 기능에 액세스할 수 있습니다. Global Accelerator는 글로벌 고객이 사용하는 인터넷 애플리케이션의

가용성과 성능을 개선하기 위해 액셀러레이터를 생성하는 네트워크 계층 서비스입니다. 자세한 내용은 [Global Accelerator](#)를 참조하세요.

AWS Managed Services FAQ의 Global Accelerator

일반적인 질문과 답변:

Q: AMS 계정에 Global Accelerator를 설정하도록 요청하려면 어떻게 해야 하나요?

AWS 서비스 RFC(관리 | AWS 서비스 | 자체 프로비저닝 서비스) 제출을 통해 액세스를 요청합니다. 이 RFC를 통해 계정에 다음 IAM 역할이 프로비저닝됩니다. `customer_global_accelerator_console_role`. 계정에 프로비저닝한 후에는 페더레이션 솔루션에서 콘솔 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Global Accelerator를 사용하는 데 따르는 제한 사항은 무엇인가요?

Global Accelerator는 리전 [AWS 테이블에](#) 나열된 여러 AWS 리전의 엔드포인트를 지원하는 글로벌 서비스입니다.

Q: AMS 계정에서 Global Accelerator를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

Global Accelerator를 사용하여 액셀러레이터를 설정할 때 정적 IP 주소를 하나 이상의 AWS 리전의 리전 엔드포인트에 연결합니다. 표준 액셀러레이터의 경우, 엔드포인트는 Network Load Balancer, Application Load Balancer, Amazon EC2 인스턴스 또는 탄력적 IP 주소입니다. 사용자 지정 라우팅 액셀러레이터의 경우 엔드포인트는 하나 이상의 EC2 인스턴스가 있는 Virtual Private Cloud(VPC) 서브넷입니다.

AMS SSP를 사용하여 AMS 계정 AWS Glue 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Glue 기능에 액세스할 수 있습니다. AWS Glue 는 분석을 위해 데이터를 준비하고 로드하는 데 도움이 되는 완전 관리형 추출, 변환 및 로드(ETL) 서비스입니다. 에서 몇 번의 클릭으로 ETL 작업을 생성하고 실행할 수 있습니다 AWS Management Console. 에 저장된 데이터를 AWS Glue 가리키면 AWS가 데이터를 AWS Glue 검색하고 관련 메타데이터(예: 테이블 정의 및 스키마)를 저장합니다 AWS Glue Data Catalog. 카탈로그가 작성되면 데이터를 즉시 검색하고 쿼리하며 ETL 작업에 사용할 수 있습니다. 자세한 내용은 [AWS Glue](#)를 참조하세요.

AWS Glue AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정에 설정 AWS Glue 하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 AWS Glue 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다.

- customer_glue_console_role
- customer_glue_service_role

앞의 역할에는 다음과 같은 연결된 정책이 포함됩니다.

- customer_glue_secrets_manager_policy
- customer_glue_deny_policy

계정에 역할이 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

크롤러, 작업 및 개발 엔드포인트(특정 사용 사례에 필요한 역할)에 액세스하려면 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 개체 또는 정책 생성(ct-3dpd8mdd9jn1r)을 사용하여 RFC를 제출합니다.

Q: AMS 계정 AWS Glue 에서 사용에 대한 제한 사항은 무엇입니까?

제한은 없습니다. 의 전체 기능은 AMS 계정에서 AWS Glue 사용할 수 있습니다. ETL 스크립트를 작성하고 테스트할 수 있는 대화형 환경의 경우 AWS Glue Studio에서 노트북을 사용합니다. AWS Glue 대화형 세션 및 작업 노트북은에서 사용할 수 AWS Glue 있고 AWS Glue 서비스 역할을 사용하는의 서버리스 기능 AWS Glue 입니다.

AWS Glue 2.0 이전: AWS Glue Notebooks는 계정에서 Amazon EC2 인스턴스를 시작하는 비관리형 리소스입니다. 자체 Amazon EC2 인스턴스를 시작하고 노트북 환경 및 개발을 지원하는 데 필요한 소프트웨어를 설치하는 것이 가장 좋습니다. 자세한 내용은 [자습서: ETL 스크립트를 테스트 및 디버깅하기 위한 로컬 Apache Zeppelin 노트북 설정](#) 및 스크립트 [개발을 위한 개발 엔드포인트 사용을 참조하세요](#).

Q: AMS 계정 AWS Glue 에서 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AWS Glue 에는 Amazon S3, CloudWatch 및 CloudWatch Logs에 대한 종속성이 있습니다. 전송 종속성은 데이터 소스에 따라 다르며 다른 AWS Glue 서비스 기능은와 상호 작용할 수 있습니다(예: Amazon Redshift, Amazon RDS, Athena).

AMS SSP를 사용하여 AMS 계정 AWS Lake Formation 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Lake Formation 기능에 액세스할 수 있습니다. AWS Lake Formation 는 며칠 내에 보안 데이터 레이크를 쉽게 설정할 수 있는 서비스입니다. 데이터 레이크는 모든 데이터를 원래 형식과 분석을 위한 형식 모두로 저장하는 큐레이팅된 중앙 집중식 보안 리포지토리입니다. 데이터 레이크를 사용하면 데이터 사일로를 분해하고 다양한 유형의 분석을 결합하여 인사이트를 얻고 더 나은 비즈니스 결정을 내릴 수 있습니다.

Lake Formation을 사용하여 데이터 레이크를 생성하는 작업은 아주 간단해서, 데이터 소스와 적용할 데이터 액세스 및 보안 정책을 정의하면 됩니다. 그런 다음 Lake Formation을 사용하여 데이터베이스 및 객체 스토리지에서 데이터를 수집하여 카탈로그화하고, 데이터를 새로운 Amazon S3 데이터 레이크로 이동하고, Machine Learning 알고리즘을 사용하여 데이터를 정리 및 분류하고, 중요한 데이터에 안전하게 액세스할 수 있습니다. 사용자는 사용 가능한 데이터 세트와 적절한 사용을 설명하는 중앙 집중식 데이터 카탈로그(자세한 내용은 [AWS Glue FAQ](#) 참조)에 액세스할 수 있습니다. 그런 다음 사용자는 Amazon [Redshift](#), [Amazon Athena](#) 및 (베타) [Amazon EMR](#) for Apache Spark와 같은 다양한 분석 및 기계 학습 서비스와 함께 이러한 데이터 세트를 활용합니다. Lake Formation은에서 사용할 수 있는 기능을 기반으로 합니다 [AWS Glue](#).

자세한 내용은 [AWS Lake Formation](#)를 참조하세요.

AWS Managed Services FAQ의 Lake Formation

Q: AMS 계정 AWS Lake Formation 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_lakeformation_data_analyst_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

또한 다음 두 가지 역할은 선택 사항입니다.

- customer_lakeformation_admin_role
- customer_lakeformation_workflow_role

관리자 권한의 경우 동일한 SSPS 변경 유형(ct-3qe6io8t6jtny)의 customer_lakeformation_admin_role 일부로 역할을 온보딩하도록 선택할 수 있습니다.

AWS Lake Formation 콘솔에서 블루프린트를 생성하려면 관리 | 기타 | 기타 RFC(ct-1e1xtak34nx76)를 제출하여 배포해야 합니다. customer_lakeformation_workflow_role. RFC에서 블루프린트가 생성될 때 버킷이 소스인 경우 S3 버킷 이름을 제공해야 합니다. S3 버킷은 블루프린트 유형이 AWS CloudTrail Classic Load Balancer Logs 또는 Application Load Balancer Logs인 경우에 적용됩니다.

Q: AMS 계정 AWS Lake Formation 에서 사용에 대한 제한 사항은 무엇인가요?

Lake Formation의 전체 기능은 AMS에서 사용할 수 있습니다.

Q: AMS 계정 AWS Lake Formation 에서 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

Lake Formation은 AWS Glue 서비스와 통합되므로 AWS Glue 사용자는 Lake Formation 권한이 있는 데이터베이스 및 테이블에만 액세스할 수 있습니다. 또한 AWS Athena 및 Amazon Redshift 사용자는 Lake Formation 권한이 있는 AWS Glue 데이터베이스와 테이블만 쿼리할 수 있습니다.

AMS SSP를 사용하여 AMS 계정 AWS Lambda 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Lambda 기능에 액세스할 수 있습니다. 서버를 프로비저닝하거나 관리하지 않고도 코드를 실행할 수 있습니다. 사용한 컴퓨팅 시간에 대해서만 비용을 지불하면 코드가 실행되지 않을 때 요금이 부과되지 않습니다. Lambda를 사용하면 사실상 모든 유형의 애플리케이션 또는 백엔드 서비스에 대한 코드를제로 관리로 실행할 수 있습니다. 코드를 업로드하면 Lambda는 고가용성으로 코드를 실행하고 확장하는 데 필요한 모든 것을 처리합니다. 코드를 설정하여 다른 AWS 서비스에서 자동으로 트리거하거나 웹 또는 모바일 앱에서 직접 호출할 수 있습니다. 자세한 내용은 [AWS Lambda](#)를 참조하세요.

AWS Managed Services FAQ의 Lambda

Q: AMS 계정 AWS Lambda 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다. customer_lambda_admin_rolecustomer_lambda_basic_execution_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Lambda 에서 사용에 대한 제한 사항은 무엇입니까?

- Lambda 함수는 이벤트 소스에서 호출하도록 설계되었습니다. Lambda 이벤트 소스로 사용할 수 있는 서비스 목록은 [다른 서비스와 AWS Lambda 함께 사용](#)을 참조하세요. 현재 AMS 계정에서 이러한 서비스를 모두 사용할 수 있는 것은 아닙니다. 사용할 수 없는 서비스가 필요한 경우 AMS CSDM과 협력하여 예외를 제출합니다.

- 기본적으로 AMS는 AWSLambdaBasicExecutionRole 및 AWSXrayWriteOnlyAccess 권한이 포함된 기본 Lambda 시작 역할을 제공합니다. 자세한 내용은 [AWS Lambda 시작 역할을 참조하세요](#). AMS VPC 내에서 Lambda 함수를 프로비저닝하는 기능과 같은 추가 권한이 필요한 경우 관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출합니다.

Q: AMS 계정 AWS Lambda 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

시작하기 위한 사전 조건이나 종속성은 없지만 AWS Lambda, 특정 사용 사례에 따라 이벤트 소스를 생성하기 위해 다른 AWS 서비스에 액세스해야 하거나 함수가 다양한 작업을 수행할 수 있는 추가 권한이 필요할 수 있습니다. 추가 권한이 필요한 경우 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(검토 필요)(ct-3qe6io8t6jtny)를 사용하여 RFC를 제출합니다.

Q: 내 계정에서 Lambda 함수를 실행하려면 어떻게 해야 하나요?

코어 계정에 Lambda 함수를 배포하려면 다음 지침을 사용합니다.

- 에 대한 SSPS AWS Lambda 가 온보딩되었는지 확인합니다.
- AMS 리소스가 보호되고 규정을 준수하는 한 AMS 책임에 따라이 배포를 금지하는 구체적인 제한은 없습니다.
- AMS가 Lambda 함수를 생성하도록 하려면 먼저 제공된 SSPS 역할을 사용해야 합니다 AWS Lambda. 그런 다음 AMS 지원이 함수를 배포하거나 지원하도록 하려면 CA에 문의하여 범위 외 (OOS) 프로세스를 시작합니다.

AMS SSP를 사용하여 AMS 계정 AWS License Manager 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS License Manager 기능에 액세스할 수 있습니다.는 AWS 서비스와 AWS License Manager 통합되어 단일 AWS 계정을 통해 여러 AWS 계정, IT 카탈로그 및 온프레미스에서 라이선스 관리를 간소화합니다.를 AWS License Manager 사용하면 관리자가 라이선스 계약 조건을 에뮬레이션하는 사용자 지정 라이선스 규칙을 생성한 다음 Amazon EC2 인스턴스가 시작될 때 이러한 규칙을 적용할 수 있습니다. 의 규칙을 AWS License Manager 사용하면 인스턴스 시작을 물리적으로 중지하거나 관리자에게 위반 사실을 알림으로써 라이선스 위반을 제한할 수 있습니다. 자세한 내용은 [AWS License Manager](#)를 참조하세요.

AWS Managed Services FAQ의 License Manager

일반적인 질문과 답변:

Q: AMS 계정에 설정 AWS License Manager 하도록 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 AWS License Manager 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_license_manager_role. License Manager IAM 역할이 계정에 프로비저닝되면 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS License Manager 에서 사용에 대한 제한 사항은 무엇인가요?

소유한 AMI에 AWS License Manager 규칙을 연결할 수 있습니다("Owned by me"에서 필터링됨). AMIs AMI에 대한 제한 연결을 적용하고(예:이 AMI의 vCPU 100개만 지원 가능) 제한을 소진하도록 선택하면 해당 AMI를 사용한 향후 시작이 차단되고 "사용 가능한 라이선스 없음"이라는 오류가 반환됩니다. 이는이 서비스의 의도된 동작입니다(라이선스 소진을 허용하지 않음). 한도를 소진했지만 AMI를 다시 시작해야 하는 경우에 구성된 규칙을 수정해야 합니다 AWS License Manager.

Q: AMS 계정 AWS License Manager 에서 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS License Manager 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Migration Hub 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Migration Hub 기능에 액세스할 수 있습니다.는 여러 AWS 및 파트너 솔루션에서 애플리케이션 마이그레이션의 진행 상황을 추적할 수 있는 단일 위치를 AWS Migration Hub 제공합니다. Migration Hub를 사용하면 요구 사항에 가장 적합한 AWS 및 파트너 마이그레이션 도구를 선택하는 동시에 애플리케이션 포트폴리오 전반의 마이그레이션 상태를 파악할 수 있습니다. 또한 Migration Hub는 마이그레이션에 사용되는 도구에 관계없이 개별 애플리케이션에 대한 주요 지표와 진행 상황을 제공합니다. 이를 통해 모든 마이그레이션에서 진행 상황을 빠르게 업데이트하고, 문제를 쉽게 식별 및 해결하며, 마이그레이션 프로젝트에 소요되는 전체 시간과 노력을 줄일 수 있습니다. 자세한 내용은 [AWS Migration Hub](#)를 참조하세요.

AWS Managed Services FAQ의 Migration Hub

일반적인 질문과 답변:

Q: AMS 계정에서 Migration Hub에 대한 액세스를 요청하려면 어떻게 해야 합니까?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Migration Hub에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_migrationhub_author_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: Migration Hub의 제한 사항은 무엇입니까?

없음.

Q: Migration Hub를 활성화하기 위한 사전 조건은 무엇입니까?

AMS 계정에서 Migration Hub 사용을 시작하기 위한 사전 조건은 없습니다. 그러나 서비스 관리 중에 서버 정보를 업로드하기 위해 Amazon S3에 권한을 쓰는 등 Migration Hub 외부의 권한이 필요할 수 있습니다.

AMS SSP를 사용하여 AMS 계정 AWS Outposts 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Outposts 기능에 액세스할 수 있습니다. AWS Outposts 는 인프라 AWS , AWS 서비스, APIs 및 도구를 사실상 모든 데이터 센터, 코로케이션 공간 또는 온프레미스 시설로 확장하여 일관된 하이브리드 환경을 제공하는 완전 관리형 서비스입니다. AWS Outposts 는 온프레미스 시스템, 로컬 데이터 처리 또는 로컬 데이터 스토리지에 대한 짧은 지연 시간 액세스가 필요한 워크로드에 적합합니다. 자세한 내용은 [AWS Outposts](#)를 참조하세요.

AWS Outposts AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정에 설정 AWS Outposts 하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC 를 AWS Outposts 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_outposts_role. 계정에 역할이 프로비저닝되면 페더레이션 솔루션에 온보딩 해야 합니다.

Q: AMS 계정 AWS Outposts 에서 사용에 대한 제한 사항은 무엇입니까?

AMS 계정 AWS Outposts 에서를 사용하는 데는 제한이 없습니다.

Q: AMS 계정 AWS Outposts 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS Outposts 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Resilience Hub 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS Resilience Hub 기능에 액세스할 수 있습니다.는 AWS 애플리케이션을 사전에 준비하고 중단으로부터 보호할 수 있도록 AWS Resilience Hub 지원합니다. Resilience Hub는 소프트웨어 개발 수명 주기에 통합되는 복원력 평가 및 검증을 제공하여 복원력 약점을 찾아냅니다. Resilience Hub는 애플리케이션이 Recovery

Time Objective(RTO) 및 Recovery Point Objective(RPO) 목표를 충족할 수 있는지 여부를 추정하고 프로덕션으로 릴리스되기 전에 문제를 해결하는 데 도움이 됩니다. AWS 애플리케이션을 프로덕션에 배포한 후 Resilience Hub를 사용하여 애플리케이션의 복원력 상태를 계속 추적할 수 있습니다. 중단이 발생하면 Resilience Hub는 운영자에게 관련 복구 프로세스를 시작하라는 알림을 보냅니다.

AWS Resilience Hub AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Resilience Hub 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Resilience Hub에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음과 같은 IAM 역할 및 정책을 프로비저닝합니다.

IAM 역할

- customer_resiliencehub_console_role
- customer_resiliencehub_service_role

정책

- customer_resiliencehub_console_policy
- customer_resiliencehub_service_policy

계정에 역할이 프로비저닝된 후 페더레이션 솔루션 customer_resiliencehub_console_role에서 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Resilience Hub 에서 사용에 대한 제한 사항은 무엇입니까?

제한은 없습니다. Resilience Hub의 전체 기능은 AMS 계정에서 사용할 수 있습니다.

Q: AMS 계정 AWS Resilience Hub 에서 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정에서 Resilience Hub를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Secrets Manager 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Secrets Manager 기능에 액세스할 수 있습니다. AWS Secrets Manager 애플리케이션, 서비스 및 IT 리소스

에 액세스하는 데 필요한 보안 암호를 보호할 수 있습니다. 이 서비스를 사용하면 수명 주기 동안 데이터베이스 자격 증명, API 키 및 기타 보안 암호를 쉽게 교체, 관리 및 검색할 수 있습니다. 사용자와 애플리케이션은 Secrets Manager APIs를 호출하여 보안 암호를 검색하므로 민감한 정보를 일반 텍스트로 하드코딩할 필요가 없습니다. Secrets Manager는 Amazon RDS, Amazon Redshift 및 Amazon DocumentDB에 대한 통합 기능이 내장된 보안 로테이션을 제공합니다. 또한 이 서비스는 API 키 및 OAuth 토큰을 비롯한 다른 유형의 보안 암호로 확장할 수 있습니다. 자세한 내용은 [AWS Secrets Manager](#)를 참조하세요.

Note

기본적으로 AMS 운영자 AWS Secrets Manager 는 계정의 기본 AWS KMS 키(CMK)를 사용하여 암호화된 보안 암호에 액세스할 수 있습니다. AMS 작업에 보안 암호에 액세스할 수 없도록 하려면 보안 암호에 저장된 데이터에 적합한 권한을 정의하는 AWS Key Management Service (AWS KMS) 키 정책과 함께 사용자 지정 CMK를 사용합니다.

AWS Managed Services FAQ의 Secrets Manager

Q: AMS 계정 AWS Secrets Manager 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출하여 Secrets Manager에 대한 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다customer_secrets_manager_console_rolecustomer-rotate-secrets-lambda-role. customer_secrets_manager_console_role는 보안 암호를 프로비저닝하고 관리하는 관리자 역할로 사용되며 보안 암호를 교체하는 Lambda 함수의 Lambda 실행 역할로 customer-rotate-secrets-lambda-role 사용됩니다. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 customer_secrets_manager_console_role 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Secrets Manager 에서 사용에 대한 제한 사항은 무엇입니까?

의 전체 기능은 보안 암호의 자동 교체 기능과 함께 AMS 계정에서 AWS Secrets Manager 사용할 수 있습니다. 그러나 '교체를 수행하기 위해 새 Lambda 함수 생성'을 사용하여 교체를 설정하는 것은 지원되지 않습니다. 변경 관리 프로세스를 우회하는 AWS CloudFormation 스택을 생성하는 데 승격된 권한(IAM 역할 및 Lambda 함수 생성)이 필요하기 때문입니다. AMS Advanced는 Lambda SSPS 관리자 역할을 사용하여 보안 암호를 교체하는 Lambda 함수를 관리하는 '기존 AWS Lambda 함수를 사용하여 교체 수행'만 지원합니다. AMS Advanced는 보안 암호를 교체하기 위해 Lambda를 생성하거나 관리하지 않습니다.

Q: AMS 계정 AWS Secrets Manager 에서 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

다음 네임스페이스는 AMS에서 사용하도록 예약되어 있으며 AWS Secrets Manager 직접 액세스의 일부로 사용할 수 없습니다.

- `arn:aws:secretsmanager:*:*:secret:ams-shared/*`
- `arn:aws:secretsmanager:*:*:secret:customer-shared/*`
- `arn:aws:secretsmanager:*:*:secret:ams/*`

Secrets Manager(AMS SSPS)를 사용하여 키 공유

RFC, 서비스 요청 또는 인시던트 보고서의 일반 텍스트로 AMS와 암호를 공유하면 정보 공개 인시던트가 발생하고 AMS는 사례에서 해당 정보를 수정하고 키를 재생성하는 요청을 수정합니다.

이 네임스페이스에서 [AWS Secrets Manager](#) (Secrets Manager)를 사용할 수 있습니다 `customer-shared`.

Secrets Manager FAQ를 사용하여 키 공유

Q: Secrets Manager를 사용하여 공유해야 하는 보안 암호 유형은 무엇입니까?

몇 가지 예는 VPN 생성을 위한 사전 공유 키, 인증 키(IAM, SSH), 라이선스 키 및 암호와 같은 기밀 키입니다.

Q: Secrets Manager를 사용하여 AMS와 키를 공유하려면 어떻게 해야 합니까?

1. 페더레이션 액세스 및 적절한 역할을 사용하여 AWS 관리 콘솔에 로그인합니다.

SALZ의 경우 `Customer_ReadOnly_Role`

MALZ의 경우 `AWSManagedServicesChangeManagementRole`.

2. [AWS Secrets Manager 콘솔](#)로 이동하여 새 보안 암호 저장을 클릭합니다.
3. 다른 유형의 보안 암호(Other type of secrets)를 선택합니다.
4. 보안 암호 값을 일반 텍스트로 입력하고 기본 KMS 암호화를 사용합니다. 다음을 클릭합니다.
5. 보안 암호 이름과 설명을 입력합니다. 이름은 항상 `customer-shared/`로 시작합니다. 예: `customer-shared/mykey2022`. 다음을 클릭합니다.
6. 자동 교체를 비활성화한 상태로 두고 다음을 클릭합니다.
7. 검토 후 저장을 클릭하여 보안 암호를 저장합니다.

8. 보안 암호를 식별하고 검색할 수 있도록 서비스 요청, RFC 또는 인시던트 보고서를 통해 보안 암호 이름으로 회신합니다.

Q: Secrets Manager를 사용하여 키를 공유하려면 어떤 권한이 필요합니까?

SALZ: customer_secrets_manager_shared_policy 관리형 IAM 정책을 찾아 정책 문서가 아래 생성 단계에 첨부된 것과 동일한지 확인합니다. 정책이 다음 IAM 역할에 연결되어 있는지 확인합니다 Customer_ReadOnly_Role.

MALZ: AMSSecretsManagerSharedPolicy가 `ams-shared` 네임스페이스에서 `GetSecretValue` 작업을 허용하는 `AWSTManagedServicesChangeManagementRole` 역할에 연결되어 있는지 확인합니다.

예시

```
{
  "Action": "secretsmanager:*",
  "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  ],
  "Effect": "Allow",
  "Sid": "AllowAccessToSharedNameSpaces"
}
```

Note

를 AWS Secrets Manager 셀프 서비스 프로비저닝된 서비스로 추가할 때 필요한 권한이 부여됩니다.

AMS SSP를 사용하여 AMS 계정 AWS Security Hub 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Security Hub 기능에 액세스할 수 있습니다.는 내의 보안 상태와 보안 업계 표준 및 모범 사례 AWS 준수에 대한 포괄적인 보기를 AWS Security Hub 제공합니다. Security Hub는 여러 AWS 계정, 서비스 및 지원되는 타사 파트너의 보안 및 규정 준수 조사 결과를 중앙 집중화하고 우선순위를 지정하여 보안 추세를 분석하고 우선순위가 가장 높은 보안 문제를 식별하는 데 도움이 됩니다. 자세한 내용은 [AWS Security Hub](#)를 참조하세요.

AWS Managed Services FAQ의 Security Hub

Q: AMS 계정 AWS Security Hub 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Security Hub에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_securityhub_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: AMS 계정에서 Security Hub를 사용하는 데 따르는 제한 사항은 무엇인가요?

아카이빙 기능은 잠재적 보안 및 운영 위험으로 기록되었으며 자체 프로비저닝된 서비스 보안 역할의 일부로 제한되었습니다.

Q: AMS 계정 AWS Security Hub 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS Security Hub 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Service Catalog AppRegistry 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AppRegistry 기능에 직접 액세스할 수 있습니다. AppRegistry를 사용하면 중앙 위치에서 애플리케이션 검색, 보고 및 관리 작업을 수행할 수 있습니다. 빌더는 단일 AWS 계정에서 애플리케이션을 거의 생성하지 않습니다. 일반적으로 개발, 테스트 및 프로덕션과 같은 수명 주기 단계에 따라 애플리케이션 리소스를 구분합니다. AppRegistry를 사용하면 정의한 AWS 계정에서 모든 리소스 컬렉션을 그룹화하고 볼 수 있습니다.

AppRegistry를 사용하면 애플리케이션, AWS 애플리케이션과 연결된 리소스 모음 및 애플리케이션 속성 그룹을 저장할 수 있습니다. 자세한 내용은 [AppRegistry란 무엇입니까?](#)를 참조하세요.

FAQ: AWS Service Catalog AppRegistry AMS

Q: AMS 계정 AWS Service Catalog AppRegistry 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 사용하여 RFC를 제출하여 AppRegistry에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer-appregistry-console-role. 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Service Catalog AppRegistry 에서 사용에 대한 제한 사항은 무엇인가요?

'Name' 태그에서 AMS 네임스페이스를 사용하는 경우를 제외하고 AppRegistry 서비스에 대한 전체 액세스 권한이 제공됩니다.

Q: AMS 계정 AWS Service Catalog AppRegistry 에서 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정에서 AppRegistry를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Shield Advanced 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Shield Advanced 기능에 액세스할 수 있습니다. AWS Shield Advanced 는에서 실행되는 애플리케이션을 보호하는 관리형 분산 서비스 거부(DDoS) 보호 서비스입니다. AWS Shield Advanced는 애플리케이션 가동 중지 시간과 지연 시간을 최소화하는 상시 감지 및 자동 인라인 완화 기능을 제공하므로 DDoS 보호의 이점을 활용하기 위해 AWS Support를 참여시킬 필요가 없습니다. AWS Shield 표준과 고급의 두 가지 티어가 있습니다. AMS는 Shield Advanced를 제공합니다. 자세한 내용은 [Shield Advanced](#)를 참조하세요.

모든 AWS 고객은 추가 비용 없이 AWS Shield Standard의 자동 보호를 이용할 수 있습니다.는 웹 사이트 또는 애플리케이션을 대상으로 하는 가장 일반적이고 자주 발생하는 네트워크 및 전송 계층 DDoS 공격으로부터 AWS Shield Standard 보호합니다. Amazon CloudFront 및 Amazon Route 53과 AWS Shield Standard 함께를 사용하면 알려진 모든 인프라(계층 3 및 4) 공격에 대한 포괄적인 가용성 보호를 받을 수 있습니다.

Amazon Elastic Compute Cloud(Amazon EC2), Elastic Load Balancing(ELB), Amazon CloudFront, AWS Global Accelerator 및 Amazon Route 53 리소스에서 실행되는 애플리케이션을 대상으로 하는 공격에 대해 더 높은 수준의 보호를 받으려면 구독하면 됩니다 AWS Shield Advanced.

와 함께 제공되는 네트워크 및 전송 계층 보호 외에도 AWS Shield Standard는 대규모의 정교한 DDoS 공격에 대한 추가 탐지 및 완화, 공격에 대한 실시간에 가까운 가시성, 웹 애플리케이션 방화벽과의 통합 AWS WAF을 AWS Shield Advanced 제공합니다. AWS Shield Advanced 또한 Amazon Elastic Compute Cloud(Amazon EC2), Elastic Load Balancing(Elastic Load Balancing), Amazon CloudFront, AWS Global Accelerator 및 Amazon Route 53 요금의 DDoS 관련 스파이크에 대한 보호 및 AWS Shield 대응 팀(SRT)에 대한 연중무휴 액세스를 제공합니다.

AWS Managed Services의 Shield Advanced FAQ

Q: AMS 계정에서 Shield Advanced에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 사용하여 RFC를 제출하여 Shield Advanced에 대한 액세스를 요청합니다. 이 RFC는 계정에 및 IAM 역할을 프로비저닝합니다 customer_shield_role aws_drt_shield_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

역할이 계정에 배포된 후를 사용하여 계정 AWS Shield Advanced 에서 customer_shield_role에 대한 구독을 확인할 수 있습니다.

Note

의 사용과 관련된 월별 요금 및 1년 약정이 있습니다 AWS Shield Advanced. 또한 AMS AWS Shield Advanced 에서 사용하면 AMS가 에스컬레이션된 분산 서비스 거부 AWS Shield (DDoS) 인시던트 중에 웹 애플리케이션 방화벽(AWS WAF) 규칙을 변경할 수 있는 (SRT)로 에스컬레이션할 수 있는 권한이 부여됩니다. 이러한 변경은 AMS와 협력하여 이루어집니다.

Q: AMS 계정에서 Shield Advanced를 사용하는 데 따르는 제한 사항은 무엇인가요?

제한은 아니지만 Shield Advanced를 사용하면 배포 aws_drt_shield_role되므로 에스컬레이션된 DDoS 인시던트 중에 AWS Shield 팀(SRT)이 AMS 계정 내부의 AWS WAF 규칙을 긴급하게 변경할 수 있습니다. 이는 DDoS 공격의 가장 빠른 문제 해결을 위해 AMS에서 권장하며 SRT로 AMS 에스컬레이션 후 발생합니다.

Q: AMS 계정에서 Shield Advanced를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정에서 Shield Advanced를 사용하기 위한 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Snowball Edge 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 Snowball Edge 기능에 직접 액세스할 수 있습니다. Snowball Edge는 안전하게 설계된 디바이스를 사용하여 AWS 클라우드 안팎으로 대량의 데이터를 전송하는 페타바이트 규모의 데이터 전송 솔루션입니다. Snowball Edge는 높은 네트워크 비용, 긴 전송 시간 및 보안 문제를 포함하여 대규모 데이터 전송과 관련된 일반적인 문제를 해결합니다. Snowball Edge를 사용하여 분석 데이터, 게놈 데이터, 비디오 라이브러리, 이미지 리포지토리, 백업을 마이그레이션하고 데이터 센터 종료, 테이프 교체 또는 애플리케이션 마이그레이션 프로젝트의 일부를 보관할 수 있습니다. Snowball Edge를 사용한 데이터 전송은 간단하고 빠르고 안전하며 고속 인터넷을 통한 데이터 전송 비용의 1/5에 불과할 수 있습니다.

Snowball Edge를 사용하면 데이터를 전송하기 위해 코드를 작성하거나 하드웨어를 구매할 필요가 없습니다. 먼저 AWS 관리 콘솔을 사용하여 Snowball용 [가져오기 작업을 생성](#)하면 Snowball 디바이스가

자동으로 배송됩니다. 디바이스가 도착하면 로컬 네트워크에 디바이스를 연결하고 Snowball 클라이언트("클라이언트")를 다운로드하여 실행하여 연결을 설정한 다음 클라이언트를 사용하여 디바이스로 전송할 파일 디렉터리를 선택합니다. 그런 다음 클라이언트는 파일을 암호화하여 디바이스에 고속으로 전송합니다. 전송이 완료되고 디바이스를 반환할 준비가 되면 E Ink 배송 레이블이 자동으로 업데이트되고 Amazon Simple Notification Service(Amazon SNS), 문자 메시지 또는 콘솔에서 직접 작업 상태를 추적할 수 있습니다. 자세한 내용은 [AWS Snowball Edge](#)를 참조하세요.

AWS Managed Services의 Snowball Edge FAQ

일반적인 질문과 답변:

Q: AMS 계정 AWS Snowball Edge 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

AMS에서 Snowball Edge 구현은 2단계 프로세스입니다.

1. 관리 제출 | 기타 | 기타 | (ct-1e1xtak34nx76) 변경 유형을 생성하고 AMS 계정의 Snowball Edge에 대한 서비스 역할을 요청합니다.
2. 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 제출하여 사용자 액세스를 요청합니다. 이 RFC는 계정에 `customer_snowball_console_role`, `customer_snowball_export_role` 및 IAM 역할을 프로비저닝합니다. `customer_snowball_import_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Snowball Edge 에서 사용에 대한 제한 사항은 무엇입니까?

의 전체 기능은 AMS 계정에서 AWS Snowball Edge 사용할 수 있습니다.

Q: AMS 계정 AWS Snowball Edge 에서을 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

위에서 언급한 대로 서비스 역할 계정이 있어야 합니다.

AMS SSP를 사용하여 AMS 계정 AWS Step Functions 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Step Functions 기능에 액세스할 수 있습니다. AWS Step Functions 는 시각적 워크플로를 사용하여 분산 애플리케이션 및 마이크로서비스의 구성 요소를 조정할 수 있는 웹 서비스입니다. 각각 기능 또는 작업을 수행하는 개별 구성 요소를 사용하여 애플리케이션을 구축하면 애플리케이션을 빠르게 확장하거나 변경할 수 있습니다. Step Functions는 구성 요소를 조정하고 애플리케이션 기능을 단계별로 실행할 수 있는 안정적인 방법을 제공합니다. Step Functions는 애플리케이션의 구성 요소를 일련의 단계로 시각화하는 그래픽 콘솔을 제공합니다. 각 단계를 자동으로 트리거 및 추적하고 오류가 있을 때 재시도하므로

애플리케이션은 매번 예상대로 순서대로 실행됩니다. Step Functions는 각 단계의 상태를 기록합니다. 따라서 무언가 잘못된 경우 빠르게 문제를 진단하고 디버깅할 수 있습니다. 자세한 내용은 [AWS Step Functions](#)를 참조하세요.

AWS Managed Services Step Functions FAQ

일반적인 질문과 답변:

Q: AMS 계정 AWS Step Functions 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC 를 AWS Step Functions 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_step_functions_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Step Functions 에서 사용에 대한 제한 사항은 무엇인가요?

의 전체 기능은 AMS 계정에서 AWS Step Functions 사용할 수 있습니다.

Q: AMS 계정 AWS Step Functions 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

런타임 시 Step Functions에서 사용하는 역할은 단계 함수에서 사용하는 서비스에 액세스할 수 있어야 합니다. 예를 들어 단계 함수는 Lambda 함수에 의존할 수 있습니다. 단계 함수를 작성하는 사람은 Lambda 함수를 동시에 생성할 가능성이 높으므로 해당 서비스에 대한 액세스도 요청해야 합니다.

AMS SSP를 사용하여 AMS 계정에서 AWS Systems Manager 파라미터 스토어 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AWS Systems Manager Parameter Store 기능에 직접 액세스할 수 있습니다. AWS Systems Manager Parameter Store는 구성 데이터 관리 및 보안 암호 관리를 위한 안전한 계층적 스토리지를 제공합니다. 암호, 데이터베이스 문자열, 라이선스 코드와 같은 데이터를 파라미터 값으로 저장할 수 있습니다. 값을 일반 텍스트 또는 암호화된 데이터로 저장할 수 있습니다. 그런 다음 파라미터를 생성할 때 지정한 고유한 이름을 사용하여 값을 참조할 수 있습니다. 확장성, 가용성 및 내구성이 뛰어난 Parameter Store는 AWS 클라우드를 기반으로 합니다. 자세한 내용은 [AWS Systems Manager 파라미터 스토어](#)를 참조하세요.

Note

수명 주기 관리가 포함된 전용 보안 암호 저장소를 원하는 경우 Parameter Store [AMS SSP](#)를 사용하여 [AMS 계정 AWS Secrets Manager 에서 프로비저닝](#) 대신을 사용합니다. Secrets

Manager를 사용하면 보안 및 규정 준수 요구 사항을 충족할 수 있으므로 보안 암호를 자동으로 교체할 수 있습니다. Secrets Manager는 Amazon RDS의 MySQL, PostgreSQL 및 Amazon Aurora에 대한 내장 통합을 제공하며, Lambda 함수를 사용자 지정하여 다른 유형의 보안 암호로 확장할 수 있습니다.

AWS Systems Manager AWS Managed Services 파라미터 스토어 FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Systems Manager Parameter Store에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 AWS Systems Manager 파라미터 스토어에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다. `customer_systemsmanager_parameterstore_console_role`. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 AWS Systems Manager 파라미터 스토어를 사용할 때 제한 사항은 무엇인가요?

AWS 관리형 키를 사용해야 합니다. 사용자 지정 KMS 키 생성은 액세스가 제한됩니다. 그러나 사용자 지정 키가 필요한 경우 RFC를 제출하여 `IAMPrincipalsRequiringDecryptPermissions` 및 `IAMPrincipalsRequiringEncryptPermissionsPrincipal` 파라미터의 `customer_systemsmanager_parameterstore_console_role` 값으로 이 IAM 역할을 사용하여 배포 | 고급 스택 구성 요소 | KMS 키 | 변경 유형 생성(ct-1d84keiri1jhg)을 사용하여 고객 관리형 키 (CMK)를 생성합니다. KMS 키가 생성된 후 이를 사용하여 보안 문자열을 생성할 수 있습니다.

Q: AMS 계정에서 AWS Systems Manager 파라미터 스토어를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

사전 조건은 없지만 SSM 파라미터 스토어는 KMS를 사용하여 보안 문자열을 생성하므로 파라미터 스토어에 저장된 값을 암호화하고 해독할 수 있습니다.

AMS SSP를 사용하여 AMS 계정에서 AWS Systems Manager 자동화 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하면 AMS 관리형 계정에서 직접 AWS Systems Manager 자동화 기능에 액세스할 수 있습니다. AWS Systems Manager 자동화는 실행서, 작업 및 서

비스 할당량을 사용하여 Amazon Elastic Compute Cloud 인스턴스 및 기타 AWS 리소스의 일반적인 유지 관리 및 배포 작업을 간소화합니다. 이를 통해 대규모로 자동화를 구축, 실행 및 모니터링할 수 있습니다. Systems Manager Automation은 Systems Manager가 관리형 인스턴스에서 수행하는 작업을 정의하는 Systems Manager 문서의 한 유형입니다. 관리형 인스턴스 내에서 명령 또는 자동화 스크립트 실행과 같은 일반적인 유지 관리 및 배포 작업을 수행하는 데 사용하는 실행서입니다. Systems Manager에는 Amazon Elastic Compute Cloud 태그를 사용하여 대규모 인스턴스 그룹을 대상으로 지정하는 데 도움이 되는 기능과 정의한 제한에 따라 변경 사항을 롤아웃하는 데 도움이 되는 속도 제어가 포함되어 있습니다. 실행서는 JavaScript Object Notation(JSON) 또는 YAML을 사용하여 작성됩니다. 그러나 Systems Manager Automation 콘솔에서 [문서 빌더(Document Builder)]를 사용하면 기본 JSON 또는 YAML로 작성하지 않고도 실행서를 생성할 수 있습니다. 또는 필요에 맞는 사전 정의된 단계가 있는 Systems Manager 제공 런북을 사용할 수 있습니다. 자세한 내용은 AWS Systems Manager 설명서의 [런북 작업을 참조하세요](#).

Note

Systems Manager Automation은 실행서에서 사용할 수 있는 20가지 작업 유형을 지원하지만, AMS Advanced 계정에서 사용할 실행서를 작성하는 동안 사용할 수 있는 작업 수는 제한적입니다. 마찬가지로 제한된 수의 Systems Manager 제공 런북을 직접 사용하거나 자체 런북 내에서 사용할 수 있습니다. 자세한 내용은 다음 FAQ의 제한 사항을 참조하세요.

AWS Systems Manager AWS Managed Services의 자동화 FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 Systems Manager Automation에 대한 액세스를 요청하려면 어떻게 해야 합니까?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 AWS Systems Manager 자동화에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다 customer_systemsmanager_automation_console_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정에서 AWS Systems Manager Automation을 사용할 때의 제한 사항은 무엇인가요?

관리형 인스턴스 내에서 명령 및/또는 스크립트만 실행하려면 자동화를 위해 제한된 Systems Manager 지원 작업 집합으로 실행서를 작성해야 합니다. 제한 사항과 함께 사용할 수 있는 작업은 다음과 같습니다.

AWS Systems Manager 자동화 제한 사항

작업	설명	제한 사항
aws:assertAwsResourceProperty –	AWS 리소스 상태 또는 이벤트 상태 어설션	EC2 인스턴스만
aws:aws:branch –	조건부 자동화 단계 실행	제한 없음
aws:createTags –	AWS 리소스에 대한 태그 생성	작성한 SSM 자동화 런북에만 해당
aws:executeAutomation –	다른 자동화 실행	작성한 자동화 실행서만
aws:executeScript –	스크립트 실행	서비스에 대한 API 호출을 수행하지 않는 스크립트만 해당
aws:pause –	자동화 일시 중지	제한 없음
aws:runCommand –	관리형 인스턴스에서 명령 실행	System Manager 제공 문서만 사용 - AWS-RunShellScript 및 AWS-RunPowerShellScript
aws:sleep –	자동화 지연	제한 없음
aws:waitForAwsResourceProperty –	AWS 리소스 속성 대기	EC2 인스턴스만

Systems Manager 콘솔에서 'Run Command' 기능을 사용하여 Systems Manager 제공 실행서 AWS-RunShellScript 및 AWS-RunPowerShellScript로 직접 명령 또는 스크립트를 실행하도록 선택할 수도 있습니다. 추가 사전 및/또는 사후 검증 또는 복잡한 자동화 로직을 지원하는 이러한 런북을 런북 내에 중첩할 수도 있습니다.

역할은 최소 권한 원칙을 준수하며 관리형 인스턴스 내에서 명령 및/또는 스크립트를 실행하기 위한 실행서의 실행 세부 정보를 작성, 실행 및 검색하는 데 필요한 권한만 제공합니다. AWS Systems Manager 서비스에서 제공하는 다른 기능에 대한 권한은 제공하지 않습니다. 이 기능을 사용하면 자동화 런북을 작성할 수 있지만 런북 실행은 AMS 소유 리소스에 대해 대상으로 지정할 수 없습니다.

Q: AMS 계정에서 AWS Systems Manager Automation을 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

사전 조건은 없지만 런북을 작성하는 동안 내부 프로세스 및/또는 규정 준수 제어를 준수해야 합니다. 또한 프로덕션 리소스에 대해 실행하기 전에 런북을 철저히 테스트하는 것이 좋습니다.

Q: Systems Manager 정책을 다른 IAM 역할에 연결할 **customer_systemsmanger_automation_policy** 수 있나요?

아니요. 다른 자체 프로비저닝 지원 서비스와 달리 이 정책은 프로비저닝된 기본 역할에만 할당할 수 있습니다 **customer_systemsmanger_automation_console_role**.

다른 SSPS 역할의 정책과 달리 이 AMS 서비스는 관리형 인스턴스 내에서 명령 또는 자동화 스크립트를 실행하기 위한 것이므로 이 SSM SSPS 정책은 다른 사용자 지정 IAM 역할과 공유할 수 없습니다. 이러한 권한을 다른 서비스에 대한 권한을 가진 다른 사용자 지정 IAM 역할에 연결할 수 있는 경우 허용된 작업 범위가 관리형 서비스로 확장되어 계정의 보안 태세가 저하될 수 있습니다.

AMS 기술 표준을 기준으로 변경 요청(RFCs)을 평가하려면 해당 클라우드 아키텍트 또는 서비스 제공 관리자와 협력하고 [RFC 보안 검토](#)를 참조하세요.

Note

AWS Systems Manager를 사용하면 계정과 공유되는 런북을 사용할 수 있습니다. 공유 런북을 사용할 때는 주의를 기울이고 실사 검사를 수행하고 콘텐츠를 검토하여 런북을 실행하기 전에 실행되는 명령/스크립트를 이해하는 것이 좋습니다. 자세한 내용은 [공유 SSM 문서의 모범 사례를 참조하세요](#).

AMS SSP를 사용하여 AMS 계정 AWS Transfer Family에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Transfer Family (Transfer Family) 기능에 액세스합니다. AWS Transfer Family는 SFTP(Secure File Transfer Protocol)를 통해 Amazon Simple Storage Service(Amazon S3) 스토리지 안팎으로 파일을 전송할 수 있는 완전 관리형 AWS 서비스입니다. SFTP는 Secure Shell(SSH) File Transfer Protocol이라고도 합니다. SFTP는 금융 서비스, 의료, 광고, 소매를 비롯한 다양한 산업의 데이터 교환 워크플로우에서 활용됩니다.

SFTP를 사용하면 서버 인프라를 실행할 필요 없이 AWS에서 SFTP 서버에 액세스할 수 있습니다. 이 서비스를 사용하여 최종 사용자의 클라이언트 및 구성을 그대로 AWS 유지하면서 SFTP 기반 워크플로를 마이그레이션할 수 있습니다. 먼저 호스트 이름을 SFTP 서버 엔드포인트와 연결한 다음 사용자를 추가하고 적절한 액세스 수준으로 프로비저닝합니다. 이렇게 하면 사용자의 전송 요청이

AWS SFTP 서버 엔드포인트에서 직접 처리됩니다. 자세한 내용은 [AWS Transfer for SFTP, SFTP 지원 서버 생성을 참조하세요](#).

AWS Transfer for SFTP AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Transfer for SFTP 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 AWS Transfer for SFTP 제출하여에 대한 액세스를 요청합니다. 이 RFC를 통해 다음 IAM 역할과 정책 이 계정에 프로비저닝됩니다.

- `customer_transfer_author_role`. 이 역할은 콘솔을 통해 SFTP 서비스를 관리하도록 설계되었습니다.
- `customer_transfer_sftp_server_logging_role`. 이 역할은 SFTP 서버에 연결되도록 설계되었습니다. 이를 통해 SFTP 서버가 CloudWatch로 로그를 가져올 수 있습니다.
- `customer_transfer_sftp_user_role`. 이 역할은 SFTP 사용자에게 연결되도록 설계되었습니다. 이를 통해 SFTP 사용자는 S3 버킷과 상호 작용할 수 있습니다.
- `policy_customer_transfer_scope_down_policy`. 이 정책은 SFTP 사용자에게 적용하여 S3 버킷에 대한 액세스를 홈 폴더로 제한할 수 있는 범위 축소 정책입니다.
- `customer_transfer_sftp_efs_user_role`. 이 역할은 SFTP 사용자에게 연결되도록 설계되었습니다. 이를 통해 SFTP 사용자는 EFS 파일 시스템과 상호 작용할 수 있습니다.

계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Transfer for SFTP 에서 사용에 대한 제한 사항은 무엇인가요?

AWS SFTP 구성을 위한 전송은 AMS 인프라에 대한 수정을 방지하기 위해 "AMS-" 또는 "MC-" 접두사가 없는 리소스로 제한됩니다.

Q: AMS 계정 AWS Transfer for SFTP 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

- AWS Transfer for SFTP 서버와 사용자를 생성하기 전에 키워드 "전송"이 포함된 이름을 가진 Amazon S3 버킷이 있어야 합니다.
- "고객 식별 공급자"를 사용하려면 API Gateway, Lambda 함수 및 사용자 리포지토리(AD, Secrets Manager 등)를 배포해야 합니다. 자세한 내용은 [AWS Transfer for SFTP 사용 및 자격 증명 공급자 작업에 대한 암호 인증 활성화 AWS Secrets Manager를 참조하세요](#).

AMS SSP를 사용하여 AMS 계정 AWS Transit Gateway 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS Transit Gateway 기능에 액세스할 수 있습니다. AWS Transit Gateway 는 Amazon Virtual Private Cloud(VPCs)와 온프레미스 네트워크를 단일 게이트웨이에 연결할 수 있는 서비스입니다. 에서 실행되는 워크로드 수가 증가함에 따라 여러 계정과 Amazon VPCs에서 네트워크를 확장하여 성장을 따라잡을 수 AWS있어야 합니다. 오늘날 피어링을 사용하여 Amazon VPCs 페어를 연결할 수 있습니다. 그러나 연결 정책을 중앙에서 관리할 수 없는 상태에서 많은 Amazon VPCs에서 point-to-point 연결을 관리하는 것은 운영 비용이 많이 들고 번거로울 수 있습니다. 온프레미스 연결을 위해 각 개별 Amazon VPC에 AWS VPN을 연결해야 합니다. 이 솔루션은 구축에 시간이 많이 걸리고 VPCs 수가 수백 개로 증가할 때 관리하기 어려울 수 있습니다. 자세한 내용은 [AWS Transit Gateway](#)를 참조하세요.

AWS Transit Gateway AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Transit Gateway 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC 를 AWS Transit Gateway 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_tgw_console_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Transit Gateway 에서 사용에 대한 제한 사항은 무엇입니까?

Transit Gateway 라우팅에 대한 라우팅 테이블 수정 AWS Transit Gateway 을 제외하고 AMS 단일 계정 랜딩 존 계정에서의 전체 기능을 사용할 수 있습니다. 관리 | 기타 | 기타 | 변경 유형 생성(ct-1e1xtak34nx76)을 제출하여 라우팅 테이블 변경을 요청합니다.

Note

이 서비스는 다중 계정 랜딩 존(MALZ)이 아닌 단일 계정 랜딩 존(SALZ)에서만 지원됩니다.

Q: AMS 계정 AWS Transit Gateway 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS Transit Gateway 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 프로비저닝 AWS WAF - AMS 계정에서 웹 애플리케이션 방화벽

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS WAF 기능에 액세스합니다. AWS WAF 는 애플리케이션 가용성에 영향을 미치거나, 보안을 손상시키거나, 과도한 리소스를 소비할 수 있는 일반적인 웹 악용으로부터 웹 애플리케이션을 보호하는 데 도움이 되는 웹 애플리케이션 방화벽(AWS WAF)입니다. AWS WAF 는 사용자 지정 가능한 웹 보안 규칙을 정의하여 웹 애플리케이션에 허용하거나 차단할 트래픽을 제어합니다. AWS WAF 를 사용하여 SQL 삽입 또는 교차 사이트 스크립팅과 같은 일반적인 공격 패턴을 차단하는 사용자 지정 규칙과 특정 애플리케이션에 맞게 설계된 규칙을 생성할 수 있습니다.

자세한 내용은 [AWS WAF - 웹 애플리케이션 방화벽](#)을 참조하세요.

AMS는에 대한 모니터링(CloudWatch 경보/이벤트/MMS 알림)을 지원하지 않습니다 AWS WAF. 의 특성으로 인해 애플리케이션에 대한 사용자 지정 규칙을 생성 AWS WAF해야 합니다. AMS는 애플리케이션의 컨텍스트 없이는 경보를 정량화하고 생성할 수 없습니다. 자세한 내용은 [AWS WAF - 웹 애플리케이션 방화벽](#)을 참조하세요.

AWS WAF AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정에 설정 AWS WAF 하도록 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC 를 AWS WAF 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝 합니다customer_waf_role. 계정에 AWS WAF IAM 역할이 프로비저닝된 후 페더레이션 솔루션에서 역할을 온보딩해야 합니다.

Q: 사용에 대한 제한 사항은 무엇입니까 AWS WAF?

권한이 프로비저닝되면의 전체 기능을 사용할 수 있습니다 AWS WAF.

Q:를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까 AWS WAF?

AMS 계정 AWS WAF 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS Well-Architected Tool 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 AWS Well-Architected Tool 기능에 직접 액세스할 수 있습니다. 는 워크로드의 상태를 검토하고 이를 최신 AWS 아키텍처 모범 사례와 비교하는 데 AWS Well-Architected Tool 도움이 됩니다. 이 도구는 클라우드 [AWS 아키텍트가 안전하고 성능이 뛰어나며 복원력이 뛰어나고 효율적인 애플리케이션 인프라를 구축할 수 있도록 개발된 Well-Architected Framework](#)를 기반으로 합니다. 이 프레임워크는 아키텍처를 평가하는 데 일관된 접근 방식을 제공하고, 솔루션 아키텍처 팀이 수행한 수만 개의 워크로드 검토에 사용되었으며, 시간이 지남에 따라 AWS 애플리케이션 요구 사항에 따라 확장되는 설계를 구현하는 데 도움이 되는 지침을 제공합니다. 자세한 내용은 [AWS Well-Architected Tool](#)를 참조하세요.

AWS WA Tool AWS Managed Services FAQ의

일반적인 질문과 답변:

Q: AMS 계정 AWS Well-Architected Tool 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 AWS Well-Architected Tool 제출하여에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_well_architected_tool_console_admin_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

Q: AMS 계정 AWS Well-Architected Tool 에서 사용에 대한 제한 사항은 무엇인가요?

의 전체 기능은 AMS 계정에서 AWS Well-Architected Tool 사용할 수 있습니다.

Q: AMS 계정 AWS Well-Architected Tool 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AMS 계정 AWS Well-Architected Tool 에서 사용할 사전 조건이나 종속성은 없습니다.

AMS SSP를 사용하여 AMS 계정 AWS X-Ray 에서 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 직접 AWS X-Ray (X-Ray) 기능에 액세스합니다. 개발자 AWS X-Ray 는 마이크로서비스 아키텍처를 사용하여 구축된 것과 같은 프로덕션 분산 애플리케이션을 분석하고 디버깅할 수 있습니다. X-Ray를 사용하면 애플리케이션과 기본 서비스가 어떻게 수행되고 있는지 이해하여 성능 문제 및 오류의 근본 원인을 식별하고 해결할 수 있습니다. X-Ray는 애플리케이션을 통해 이동하는 요청에 대한 end-to-end 보기를 제공하고 애플리케이션

이션의 기본 구성 요소 맵을 보여줍니다. X-Ray를 사용하여 간단한 3계층 애플리케이션에서 수천 개의 서비스로 구성된 복잡한 마이크로서비스 애플리케이션에 이르기까지 개발 중인 애플리케이션과 프로덕션 중인 애플리케이션을 모두 분석할 수 있습니다. 자세한 내용은 [AWS X-Ray](#)를 참조하세요.

AWS Managed Services FAQ의 X-Ray

일반적인 질문과 답변:

Q: AMS 계정 AWS X-Ray 에서에 대한 액세스를 요청하려면 어떻게 해야 하나요?

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 변경 유형을 제출하여 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 역할을 프로비저닝합니다customer_xray_console_role. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다. 또한 Amazon EC2 인스턴스에서 X-Ray로 데이터를 푸시customer_xray_daemon_write_instance_profile하려면가 있어야 합니다. 이 인스턴스 프로파일은를 수신할 때 생성됩니다customer_xray_console_role.

AMS Operations에 서비스 요청을 제출하여 기존 인스턴스 프로파일에customer_xray_daemon_write_policy를 할당하거나 AMS Operations가 X-Ray를 활성화할 때 생성된 인스턴스 프로파일을 사용할 수 있습니다.

Q: AMS 계정 AWS X-Ray 에서 사용에 대한 제한 사항은 무엇인가요?

AWS KMS 키(KMS 키)를 사용한 암호화를 제외하고 AMS 계정에서의 전체 기능을 사용할 수 있습니다. AWS X-Ray 는 기본적으로 모든 추적 데이터를 AWS X-Ray 암호화합니다. 기본적으로 X-Ray 는 추적 및 관련 저장 데이터를 암호화합니다. 키로 저장 데이터를 암호화해야 하는 경우 AWS관리형 KMS 키(aws/xray) 또는 KMS 고객 관리형 키를 선택할 수 있습니다. X-Ray 암호화를 위한 KMS 고객 관리형 키의 경우 관리 | 기타 | 기타 | 변경 유형 생성(ct-1e1xtak34nx76)을 제출합니다.

Q: AMS 계정 AWS X-Ray 에서를 사용하기 위한 사전 조건 또는 종속성은 무엇입니까?

AWS X-Ray 에는 AMS 계정에 이미 구현된 Amazon S3, CloudWatch 및 CloudWatch Logs에 대한 종속성이 있습니다. 전송 종속성은 데이터 소스 및 기능이 상호 작용할 수 AWS X-Ray 있는 기타 AWS 서비스(예: Amazon Redshift, Amazon RDS, Athena)에 따라 달라집니다.

AMS SSP를 사용하여 AMS 계정에서 VM Import/Export 프로비저닝

AMS 셀프 서비스 프로비저닝(SSP) 모드를 사용하여 AMS 관리형 계정에서 VM 가져오기/내보내기 기능에 직접 액세스할 수 있습니다. VM Import/Export를 사용하면 기존 환경에서 Amazon EC2 인스턴스

로 가상 머신 이미지를 쉽게 가져와 온프레미스 환경으로 다시 내보낼 수 있습니다. 이 제품을 사용하면 IT 보안, 구성 관리 및 규정 준수 요구 사항을 충족하도록 구축한 가상 머신에 대한 기존 투자를 즉시 ready-to-use 수 있는 인스턴스로 Amazon EC2로 가져와 활용할 수 있습니다. 가져온 인스턴스를 온프레미스 가상화 인프라로 다시 내보내 IT 인프라 전체에 워크로드를 배포할 수도 있습니다. 자세한 내용은 [VM Import/Export](#)를 참조하세요.

AWS Managed Services의 VM Import/Export FAQ

일반적인 질문과 답변:

Q: AMS 계정에서 VM Import/Export에 대한 액세스를 요청하려면 어떻게 해야 하나요?

관리 | AWS 서비스 | 자체 프로비저닝 서비스 | 변경 유형 추가(ct-1w8z66n899dct)를 사용하여 RFC를 제출하여 VM Import/Export에 대한 액세스를 요청합니다. 이 RFC는 계정에 다음 IAM 정책을 프로비저닝합니다 customer_vmimport_policy. 계정에 프로비저닝된 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.

서비스가 계정에서 작업을 수행하려면 추가 역할인 VM Import/Export Service 역할이 필요합니다.

Q: AMS 계정에서 VM Import/Export를 사용할 때 제한 사항은 무엇인가요?

- 사용자 지정 머신 이미지와 데이터 볼륨을 가져오는 기능은 모두 AMS VM Import/Export에서 사용할 수 있습니다. 그러나 S3에 대한 권한은 계정 내 정보에 대한 액세스를 제한하기 customer-vmimport-* 위해 이름과 일치하는 버킷으로 작업을 제한하도록 범위가 축소되었습니다.
- 이미지 및 스냅샷 가져오기는 AMS VM Import/Export에서 지원됩니다. 그러나 보안 조치로 인해 인스턴스 가져오기 및 인스턴스 내보내기 기능을 사용할 수 없습니다.
- 또한 제한 및 민감한 데이터를 내보낼 위험을 완화하기 위해 내보내기 기능이 비활성화되었습니다.

Q: AMS 계정에서 VM Import/Export를 사용하기 위한 사전 조건 또는 종속성은 무엇인가요?

- AWS 환경으로 가져오려면 지원되는 디스크 이미지를 제공해야 합니다. 자세한 내용은 [VM Import/Export Requirements](#)를 참조하세요.
- AWS 콘솔을 통해 VM Import/Export에 액세스할 수 없습니다. AWS CLI AWS Tools for PowerShell 또는 AWS SDKs를 통해이 서비스에 액세스해야 합니다. 또는 변경 유형 ct-117rmp64d5mvp: 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | EC2 인스턴스 프로파일 생성을 제출하여 인스턴스 프로파일을 요청할 수 있습니다. 이 인스턴스 프로파일을 사용하면 도구가 인스턴스에서 명령을 수행할 수 있습니다.

고객 관리형 모드

AWS Managed Services(AMS) 고객 관리형 모드는 유연한 거버넌스 모델을 제공하며 요구 사항에 맞게 조정할 수 있습니다. 이는 AMS가 작동하지 않는 서비스 및 애플리케이션에 대한 대체 옵션으로 간주될 수 있습니다. AMS는 이 모드에서 생성된 계정에서 호스팅되는 인프라를 운영하지 않습니다. 그러나 이 모드에서 중앙 집중식 다중 계정 관리를 활용할 수 있습니다. 이 모드에서는 다음과 같은 다중 계정 랜딩 존 기능을 활용할 수 있습니다.

- 자동 계정 배포
- 네트워킹 계정의 Transit Gateway를 통한 연결
- AMS Config 규칙 라이브러리
- 로그 복사본을 로깅 계정에 저장
- 보안 계정에 대한 고객 관리형 Guard Duty 알림 집계
- 통합 결제
- 사용자 지정 서비스 제어 정책 활성화.

예: AMS에서 관리하는 운영 체제가 아닌 Ubuntu Pro에서 워크로드를 실행하려는 경우 고객 관리형 계정을 사용하여 호스팅할 수 있습니다. 고객 관리형 계정을 통해 워크로드를 통합하여 AWS 조직 간 공유를 통해 사용할 수 있는 예약 인스턴스/공유 플랜에 대한 대량 할인을 활용할 수도 있습니다.

고객 관리형 모드 시작하기

AMS 고객 관리형 모드는 특수 다중 계정 랜딩 존 애플리케이션 계정을 통해 사용할 수 있습니다.

고객 관리형 애플리케이션 계정을 생성하는 방법을 비롯한 자세한 내용은 [고객 관리형 애플리케이션 계정을](#) 참조하세요.

AMS 및 AWS Service Catalog

AWS Managed Services(AMS)의 Service Catalog를 사용하면 조직이 AWS IT(정보 기술) 서비스의 카탈로그를 생성 및 관리할 수 있으며, IT 관리자는 승인된 제품의 카탈로그를 생성 및 관리하고 계정의 최종 사용자에게 배포하여 맞춤형 서비스 포털에서 필요한 제품에 액세스할 수 있습니다. 관리자는 각 제품에 액세스할 수 있는 사용자를 제어하여 조직 비즈니스 정책을 준수할 수 있습니다. 관리자는 최종 사용자가 승인된 리소스를 배포하기 위해 Service Catalog에 대한 IAM 액세스만 요구하도록 역할을 설정할 수도 있습니다. Service Catalog를 사용하면 조직이 민첩성을 높이고 비용을 절감할 수 있습니다. 최종 사용자는 사용자가 제어하는 카탈로그에서 필요한 제품만 찾아 시작할 수 있기 때문입니다.

Service Catalog는 AMS 관리형 계정(들)에서 리소스를 프로비저닝하고 업데이트하기 위한 AMS 변경 요청(RFC) 프로세스의 대안을 제공합니다. AMS는 보안, 규정 준수, 프로비저닝, 가용성, 패치, 모니터링, 알림, 보고, 인시던트 대응, 비용 최적화를 포함하여 Service Catalog를 통해 프로비저닝된 모든 인프라 리소스에 대해 대규모로 AWS를 실행하는 데 필요한 모든 인프라 운영 작업을 관리합니다. AMS 관리형 계정에서 Service Catalog를 활용하면 일반적으로 배포되는 IT 서비스를 중앙에서 관리하고 일관된 거버넌스를 달성하는 동시에 사용자가 필요한 승인된 IT 서비스만 관리형 환경에 빠르게 배포할 수 있습니다.

Service Catalog 시작하기

AMS에서 Service Catalog를 시작하려면 AMS 콘솔을 통해 서비스 요청을 제출하여 Service Catalog에 대한 액세스를 요청합니다. 요청을 제출하면 AMS(이전에 Transform 설명됨)를 호출하는 CloudFormation 매크로가 포함된 AMS 관리형 스택과 함께 세 개의 IAM 역할이 계정에 배포되어 시스템에 제품을 등록하고 Service Catalog를 통해 프로비저닝된 인프라에 대해 작업을 수행할 수 있습니다. 배포된 세 가지 IAM 역할에는 IT 관리자가 제품을 Service Catalog 관리자로 관리하는 역할, 애플리케이션 소유자와 최종 사용자가 제품을 구성, 시작 및 관리하는 역할, Service Catalog가 제품을 시작하거나 업데이트하는 동안 사용할 권한을 정의하는 시작 제약 조건으로 사용할 역할이 포함됩니다.

시작하기 전에 AMS의 Service Catalog

Service Catalog가 기존 AMS 변경 요청(RFC) 프로세스를 대체하나요?

Service Catalog가 활성화된 계정에서는 사전 정의된 제품 카탈로그를 통해 AMS 계정에서 IT 서비스를 프로비저닝하고 업데이트하는 변경 관리 시스템 역할을 합니다. AMS는 기본 포트폴리오/제품 카탈로그를 제공하며 IT 관리자는 직접 생성하고 구성할 수 있습니다. Service Catalog는 Service Catalog를 통해 프로비저닝된 스택만 승인합니다. 마찬가지로 Service Catalog 외부에서 수정하면 승인된 제품 구성에서 스택이 드리프트되므로 Service Catalog를 통해 프로비저닝된 서비스는 AMS RFC 프로세스를 통해 수정할 수 없습니다.

AMS 콘솔에서 서비스 카탈로그를 통해 프로비저닝된 스택을 볼 수 있나요?

예. AMS 콘솔에서 서비스 카탈로그를 통해 프로비저닝된 모든 스택을 볼 수 있습니다. 서비스 카탈로그를 통해 프로비저닝된 스택은 스택 ID "SC-"로 쉽게 식별할 수 있습니다. 스택은 AMS 콘솔에서 볼 수 있지만 AMS RFC 프로세스를 통해 업데이트할 수 없습니다. AMS 변경 관리 시스템(RFCs)에 대한 액세스는 액세스 요청, 패치 오케스트레이션 및 백업 RFCs로만 제한됩니다.

Service Catalog를 통해 스택을 프로비저닝 및/또는 업데이트하면 AMS 콘솔에 해당 RFC가 있습니까?

AMS 콘솔에 표시되는 유일한 RFC는 스택이 처음 프로비저닝될 때 AMS에 스택을 등록하는 RFC입니다. 이 RFC는 Service Catalog를 통해 스택이 시작될 때 트리거되는 AMS 검증 프로세스에 의

해 자동으로 제출됩니다. 다른 모든 프로비저닝 및 변경 사항은 Service Catalog에서 직접 추적되며 Service Catalog 콘솔에서 볼 수 있습니다. 또한 Service Catalog의 프로비저닝된 제품 계획 기능을 사용하여 제품을 프로비저닝하거나 업데이트하기 전에 리소스에 적용될 변경 사항 목록을 볼 수 있습니다.

AMS 관리형 계정에서 제품을 프로비저닝할 때 특정 작업을 수행해야 합니까?

예. AMS 계정에 프로비저닝된 모든 Service Catalog 제품은 해당 제품을 정의하는 CFN 템플릿에 다음 JSON 행을 포함해야 합니다.

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

이 CloudFormation 코드 조각은 AMS 관리형 계정에서 리소스를 프로비저닝하기 위해 필요한 AMS 검증을 트리거합니다. 이 코드 줄을 제품 정의의 일부로 포함하는 것은 사용자의 책임입니다. 포함되지 않은 경우 프로비저닝이 실패하고 "Failed to create product. 이 계정은 AMS에서 관리합니다. AMS 계정의 모든 제품은 템플릿에 AMS Transform 코드가 있어야 합니다."

시작 시 AMS 고객이 사용할 수 없거나 제한되는 Service Catalog 기능이 있나요?

예, 초기 시작 시 AMS 고객은 다음 SC 기능을 사용할 수 없습니다.

- Service Catalog를 통한 계정 생성
- Service Catalog를 통해 AMS 관리형 계정으로 모든 AWS 서비스를 시작할 수 있습니다. AWS 서비스 가용성은 AMS 지원 서비스(관리형 및 자체 프로비저닝형)로 제한됩니다. AMS 지원 서비스에 대한 자세한 내용은 AMS 서비스 설명을 참조하세요.
- Service Catalog IT 서비스 관리자(ITSM) 커넥터는 AMS 인시던트 보고서 및 서비스 요청과 통신하지 않습니다.
- Service Catalog 빠른 시작을 활용하고 수정 없이 아키텍처를 참조할 수 있습니다. AMS 계정용 Service Catalog 제품에는 다음 JSON 코드 행이 포함되어야 합니다.

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

CNF 템플릿의 . 이 줄은 일반적인 AWS CloudFormation 템플릿의 일부가 아니므로 명시적으로 추가해야 합니다.

- Terraform은 현재 Service Catalog 제품 프로비저닝을 위해 AMS에서 지원되지 않습니다.
- AWS CFN 스택 세트는 AMS에서 지원되지 않습니다.
- 사용자 지정 IAM 역할은 생성할 수 없습니다.

- 서비스 작업은 다음으로 제한됩니다.

- [AWS-RebootRdsInstance](#)
- [AWS-RestartEC2Instance](#)
- [AWS-StartEC2Instance](#)
- [AWS-StartRdsInstance](#)
- [AWS-StopEC2Instance](#)
- [AWS-StopRdsInstance](#)
- [AWS-CreatelImage](#)
- [AWS-CreateRdsSnapshot](#)
- [AWS-CreateSnapshot](#)

 Note

서비스 작업을 생성할 때 최종 사용자의 권한, 시작 역할 또는 선택한 사용자 지정 IAM 역할로 실행 역할을 구성할 수 있습니다. 선택한 실행 역할에는 서비스 작업을 수행할 수 있는 충분한 권한이 있어야 하며 서비스 카탈로그에서 수입할 수 있는 TrustPolicy가 있어야 합니다. 그렇지 않으면 실행 시 해당 서비스 작업이 실패합니다. 서비스 작업으로 사용할 올바른 권한과 신뢰 정책이 있는 AWSManagedServicesServiceCatalogLaunchRole을 사용하는 것이 좋습니다.

AMS RFC 시스템을 계속 사용해야 하는 대상은 무엇입니까?

일반 가용성(GA)에서도 RFCS를 사용하여 다음 작업을 실행해야 합니다.

- 패치 오케스트레이터 구성
- 백업 정책 구성
- 인스턴스 액세스 요청
- AMS 지침을 벗어나는 보안 그룹 생성 및 할당.
- 워크로드 수집 수행(WIGS)
- IAM 역할 생성

Service Catalog CLI를 사용하여 AMS 관리형 계정의 Service Catalog에 액세스할 수 있나요?

예, Service Catalog APIs CLI를 통해 사용 및 활성화됩니다. 해당 아티팩트의 프로비저닝 및 종료 를 통해 Service Catalog 아티팩트 관리의 작업을 사용할 수 있습니다. 자세한 내용은 [AWS Service Catalog 리소스](#)를 참조하거나 최신 AWS SDK 또는 CLI를 다운로드하세요.

누가 고객의 승인된 제품 카탈로그를 생성, 관리 및 배포하나요?

고객의 카탈로그 관리자 및/또는 IT 관리자 또는 할당된 리소스는 서비스 카탈로그 카탈로그 및 승인된 제품의 관리를 담당합니다.

AMS AMIs 사용할 수 있나요?

2020년 3월 이후에 판매된 AMS AMIs는 AWS Service Catalog를 통해 배포할 수 있습니다.

Service Catalog를 사용하여 AMS로 마이그레이션하려면 어떻게 해야 하나요?

Service Catalog를 사용하여 워크로드를 AMS로 마이그레이션하려면 먼저 [워크로드 수집\(WIGs\)](#) 프로세스에 따라 AMS에서 AMI를 생성합니다. WIGS에서 생성한 AMI를 사용하여 Service Catalog에서 제품을 생성합니다. 이 작업을 수행하는 방법은 [AWS Service Catalog - 시작하기에 자세히 설명되어 있습니다](#).

필요한 데이터 찾기(SKMS), AMS

AWS Managed Services(AMS) 계정을 사용할 때 필요한 데이터를 찾으려면 AMS 서비스 지식 관리 또는 SKMS 시스템에서 호출합니다. AMS.

SKMS는 서비스 지식 관리 시스템을 의미하며 고객을 위한 AWS Managed Services(AMS) 서비스와 관련된 모든 정보를 나타냅니다. AMS에는 데이터를 찾기 위한 SKMS API가 있습니다.

주제

- [서비스 지식 관리란 무엇입니까?](#)
- [AMS에서 VPC IDs 찾기](#)
- [AMS에서 서브넷 IDs 찾기](#)
- [AMI IDs AMS 찾기](#)
- [보안 그룹\(SG\) IDs, AMS 찾기](#)
- [AMS에서 IAM 엔터티 찾기](#)
- [AMS에서 스택 IDs 찾기](#)
- [AMS에서 인스턴스 IDs 또는 IP 주소 찾기](#)
- [AMS에서 Amazon 리소스 이름\(ARNs\) 찾기](#)
- [AMS에서 ARN으로 리소스 찾기](#)
- [AMS 계정 설정 찾기](#)

서비스 지식 관리란 무엇입니까?

서비스 지식 관리는 AMS 계정의 모든 정보를 저장하는 것입니다. 다음에 대한 정보는 AMS 서비스 지식 관리 시스템(SKMS), AMS SKMS API 또는 AMS 콘솔을 통해 얻을 수 있습니다.

- VPC
- 관리형 서브넷
- Amazon EC2 인스턴스 및 기타 리소스를 포함한 스택 및 스택 구성 요소
- Amazon Machine Images(AMI)

SKMS의 정보를 사용하여 관리 중인 인프라를 이해하고 인프라를 생성, 변경 또는 제거하기 위한 변경 관리 및 서비스 요청을 위한 입력으로 사용할 수 있습니다.

Note

모든 AMS SKMS API 호출이에 기록됩니다 AWS CloudTrail.

환경(VPCs 및 서브넷) 및 해당 환경에 배포할 수 있는 애플리케이션 리소스(스택, Amazon EC2 인스턴스, 인스턴스 이미지 또는 AMIs)에 대한 정보를 검색하는 작업을 제공하는 AMS SKMS API를 통해 SKMS에 액세스합니다.

VPCs 및 인스턴스 이미지는 온보딩 중에 필요한 액세스 권한을 사용하여 계정에 설정됩니다. 설정이 완료되면 변경 관리 시스템을 사용하여 VPCs를 작업 스택으로 채울 수 있습니다.

AMS에서 VPC IDs 찾기

Virtual Private Cloud(VPC)에는 하나 이상의 서브넷이 있습니다. AMS에서 VPC에는 AWS 리전 있으며 프라이빗 및 퍼블릭 서브넷이 있습니다.

또한 [AMS에서 서브넷 IDs 찾기](#) 섹션도 참조하세요.

일부 CTs VpcId가 필요합니다. VPC ID를 찾으려면 AMS 콘솔 또는 API/CLI를 사용할 수 있습니다.

AMS 콘솔:

탐색 창에서 VPCs 및 관련 VPC를 선택합니다. 선택한 VPC의 VPC 세부 정보 페이지가 VPC ID를 포함한 정보와 함께 열립니다.

AMS SKMS API ListVpcSummaries 또는 CLI:

Note

이러한 명령이 작동하려면 AMS CLI가 설치되어 있어야 합니다. AMS API 또는 CLI를 설치하려면 AMS 콘솔 개발자 리소스 페이지로 이동합니다. AMS CM API 또는 AMS SKMS API에 대한 참조 자료는 사용 설명서의 AMS 정보 리소스 섹션을 참조하세요. 인증 `--profile` 옵션을 추가해야 할 수 있습니다. 예: `aws amsskms ams-cli-command --profile SAML`. 와 같이 모든 AMS 명령이 us-east-1에서 부족하므로 `--region` 옵션을 추가해야 할 수도 있습니다 `aws amscm ams-cli-command --region=us-east-1`.

Note

AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다. us-east-1. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 --region us-east-1 때를 추가해야 할 수 있습니다. 인증 방법인 --profile saml 경우를 추가해야 할 수도 있습니다.

1. 다음 예제에서 첫 번째 명령은 계정의 모든 VPCs에 대한 요약 목록을 요청합니다. 두 번째 명령은 2016년에 생성된 VPCs만 나열하고 CreatedTime, VpcId 및 이름을 출력하기 위해 쿼리 필터와 함께 VPCs 목록을 요청합니다.

Note

AMS 콘솔의 개발자 리소스 페이지를 통해 AMS SKMS CLI를 가져올 수 있습니다.

```
aws amsskms list-vpc-summaries --output table
```

```
-----
|                               ListVPCSummaries                               |
+-----+
|                               VPCSummaries                                |
|+-----+-----+
| CreatedTime      | 2016-01-15T18:50:11Z |
| VpcId            | vpc-01234567890abcdef |
| LastModifiedTime | 2016-01-15T18:50:11Z |
| Name             | 952444781316-initial-vpc |
|+-----+-----+
|                               Visibility                                |
|+-----+-----+
| Id               | PrivateAndPublic      |
| Name             | PrivateAndPublic      |
|+-----+-----+
```

2. 이번에는 쿼리가 있습니다.

```
aws amsskms list-VPC-summaries --query "VPCSummaries[?
starts_with(@.CreatedTime,to_string(`2016`))].[CreatedTime, VpcId, Name]" --output
table
```

```
-----
|                                     ListVPCSummaries                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|2016-01-15T18:50:11Z | vpc-01234567890abcdef | 952444781316-initial-VPC |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

AMS에서 서브넷 IDs 찾기

여러 리소스에서는 구성 시 서브넷 또는 서브넷 목록을 지정해야 합니다. 서브넷을 찾으려면 AMS 콘솔 또는 AMS SKMS API/CLI를 사용할 수 있습니다. AMS SKMS API/CLI는 프라이빗이며 사용하기 전에 설치해야 합니다.

AMS 콘솔:

1. 탐색 창에서 VPCs 및 관련 VPC를 선택합니다. 선택한 VPC의 VPC 세부 정보 페이지가 서브넷 테이블과 함께 열리고 서브넷 ID를 클릭하여 세부 정보 페이지를 열고 ID를 찾습니다.

AMS SKMS API ListSubnetSummaries 또는 CLI:

Note

이러한 명령이 작동하려면 AMS CLI가 설치되어 있어야 합니다. AMS API 또는 CLI를 설치하려면 AMS 콘솔 개발자 리소스 페이지로 이동합니다. AMS CM API 또는 AMS SKMS API에 대한 참조 자료는 사용 설명서의 AMS 정보 리소스 섹션을 참조하세요. 인증 `--profile` 옵션을 추가해야 할 수 있습니다. 예: `aws amsskms ams-cli-command --profile SAML`.와 같이 모든 AMS 명령이 `us-east-1`에서 실행되므로 `--region` 옵션을 추가해야 할 수도 있습니다. `aws amscm ams-cli-command --region=us-east-1`.

Note

AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다. us-east-1. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 --region us-east-1 때를 추가해야 할 수 있습니다. 인증 방법인 --profile saml 경우를 추가해야 할 수도 있습니다.

VPC의 서브넷을 찾으려면 다음과 같이 list-subnet-summaries 명령을 사용하여 검색할 수 있습니다.

Note

AMS 계정에 없는 서브넷을 찾는 경우를 시도할 수 있습니다. aws ec2 describe-subnets --region us-west-2.

1. SKMS API/CLI ListSubnetSummaries 작업:

간단한 목록:

```
aws amsskms list-subnet-summaries
```

테이블에 대한 출력:

```
aws amsskms list-subnet-summaries --output table
```

2. SKMS API ListSubnetSummaries 작업에는 가시성에 따라 결과의 범위를 좁히는 파라미터가 있습니다. 또한 이름을 기준으로 결과를 [필터링](#)할 수 있습니다. CLI를 사용하는 경우 --query 옵션을 사용하여 출력 범위를 좁히거나 값의 일부를 검색할 수도 있습니다. 예를 들어 특정 VPC의 모든 서브넷을 찾으려면 다음 명령을 사용할 수 있습니다.

```
aws amsskms list-subnet-summaries --query
"SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

다음과 같이 반환됩니다.

```
-----
```

ListSubnetSummaries			
Visibility	SubnetId	Name	
Private	subnet-01234567890abcdef	Demo Deployment Zone #1	
Private	subnet-01234567890abcdef	Demo Deployment Zone #1	
Public	subnet-01234567890abcdef	Demo DMZ #1	
Public	subnet-01234567890abcdef	Demo DMZ #1	

CLI 쿼리 사용에 대한 자세한 내용은 [--query 옵션을 사용하여 출력을 필터링하는 방법](#) 및 쿼리 언어 참조인 [JMESPath 사양](#)을 참조하세요.

- VPCs가 여러 개 있는 경우 명령에 VPC 필터를 포함시킨 다음 각 VPC에 대해 명령을 실행합니다.
예:

```
list-subnet-summaries --filter Attribute=VpcId,Value=vpc-xxxxxxx --query
"SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

- AWS에서는 [describe-subnets](#)를 사용합니다.

CLI 쿼리 사용에 대한 자세한 내용은 [--query 옵션을 사용하여 출력을 필터링하는 방법](#) 및 쿼리 언어 참조인 [JMESPath 사양](#)을 참조하세요.

서브넷 이름

사용자로부터 입력을 수집하여 시스템에 추가하면 AMS 서브넷이 자동으로 생성됩니다. AMS는 수식을 사용하여 **AACCOUNT_ID-SUBNET-TYPE-AZ-IDENTIFIER**라는 서브넷 이름을 생성합니다. 서브넷 유형은 dmz, shared-services 또는 customer-application입니다. 고객 애플리케이션 서브넷이 두 개 이상인 경우 계정 ID 뒤에 서브넷이 "추가" 또는 "예약" 서브넷임을 나타내는 선택적 식별자가 서브넷 이름에 추가될 수 있습니다.

AMI IDs AMS 찾기

Amazon Machine Image 또는 AMI는 Amazon EC2 인스턴스에서 생성된 Amazon EC2 인스턴스용 템플릿입니다.는 매달 업데이트된 AMIs(예: 패치 포함)를 AWS 제공하지만 AWS Managed Services(AMS)에는 AMS 사용을 위해 수정된 AMIs 필요합니다. AMS는 매월 패치 화요일 직후 사용할 수 있는 새 AMIs를 릴리스합니다.

Amazon Machine Image(AMIs)는 AWS에서 EC2 인스턴스를 생성하는 데 사용되는 인스턴스 구성 템플릿입니다. AMS에서는 AMS 관리형 리소스에 특정 AMIs 사용해야 합니다. EC2 인스턴스 및 EC2

Auto Scaling 그룹을 생성하기 위한 변경 유형을 사용하려면 변경 유형이 생성하는 인스턴스의 기반으로 사용할 AMS용 AMI를 지정해야 합니다. AMS에서는 항상 사용 가능한 최신 AMI를 선택할 것을 권장합니다.

AWS AMIs. [AWS](#)

AMS 계정에 대한 Amazon EC2 스택 또는 Amazon EC2 Auto Scaling 그룹을 생성할 때 Amild를 지정해야 합니다. "customer-"로 시작하는 AMIs로 제한되며 항상 최신 AMI를 선택하는 것이 좋습니다.

계정의 최신 AMI를 찾으려면 AMS SKMS CLI 명령으로 검색하거나 AMS 콘솔 세부 정보 페이지에서 관련 VPC를 사용할 수 있습니다.

- AMS 콘솔 사용: 사용 가능한 AMIs는 AMS 콘솔의 AMI 페이지에 나열됩니다. 이름이 "customer-"로 시작하는 AMIs 중에서 선택합니다.
- AMS SKMS API/CLI ListAmis 작업을 사용합니다.

Note

이러한 명령이 작동하려면 AMS CLI가 설치되어 있어야 합니다. AMS API 또는 CLI를 설치하려면 AMS 콘솔 개발자 리소스 페이지로 이동합니다. AMS CM API 또는 AMS SKMS API에 대한 참조 자료는 사용 설명서의 AMS 정보 리소스 섹션을 참조하세요. 인증 --profile 옵션을 추가해야 할 수 있습니다. 예: `aws amsskms ams-cli-command --profile SAML`. 와 같이 모든 AMS 명령이 us-east-1에서 부족하므로 --region 옵션을 추가해야 할 수도 있습니다 `aws amscm ams-cli-command --region=us-east-1`.

다음은 결과를 고객 AMI로 제한하는 query 옵션이 있는 CLI 예제입니다. AMIs

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --output table
```

이 예제에서는 filter 옵션과 함께 query 옵션을 사용하여 "customer"로 시작하는 Windows AMIs 찾습니다.

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --filter Attribute=Platform,Value=windows --output table
```

- CLI 쿼리 사용에 대한 자세한 내용은 [--query 옵션을 사용하여 출력을 필터링하는 방법](#) 및 쿼리 언어 참조인 [JMESPath 사양](#)을 참조하세요.

보안 그룹(SG) IDs, AMS 찾기

Amazon EC2 생성 및 OpenSearch 생성 도메인 CTs 보안 그룹 ID가 필요합니다. 형식입니다sg-02ce123456e7893c7. 계정에 기본 보안 그룹이 두 개 이상 있습니다. 섹션을 참조하세요[보안 그룹](#). 또한 특정 목적으로 생성한 보안 그룹이 있을 수 있습니다. 보안 그룹을 검색하려면:

- AWS 콘솔: EC2 또는 VPC 콘솔을 사용하여 선택한 VPC의 모든 보안 그룹을 봅니다.
- API/CLI(AMS 계정에 로그인한 경우):

보안 그룹을 나열합니다.

```
aws ec2 describe-security-groups
```

AMS에서 IAM 엔터티 찾기

계정에는 기본 IAM 역할 및 정책이 있습니다. 및 기본 IAM 인스턴스 프로파일은 섹션을 참조[AMS의 IAM 사용자 역할](#) 하고, 기본 정책은 [EC2 IAM 인스턴스 프로파일](#) 섹션을 참조하세요. IAM 역할 및 정책을 검색하려면:

- 콘솔: IAM 콘솔을 사용하여 계정의 모든 IAM 정책 및 역할을 봅니다.
- API/CLI(AMS 계정에 로그인한 경우):

Note

이러한 명령이 작동하려면 AMS CLI가 설치되어 있어야 합니다. AMS API 또는 CLI를 설치하려면 AMS 콘솔 개발자 리소스 페이지로 이동합니다. AMS CM API 또는 AMS SKMS API에 대한 참조 자료는 사용 설명서의 AMS 정보 리소스 섹션을 참조하세요. 인증 --profile 옵션을 추가해야 할 수 있습니다. 예: `aws amsskms ams-cli-command --profile SAML`. 와 같이 모든 AMS 명령이 us-east-1에서 부족하므로 --region 옵션을 추가해야 할 수도 있습니다`aws amscm ams-cli-command --region=us-east-1`.

역할을 나열합니다.

```
aws --profile saml iam list-roles
```

정책을 나열합니다.

```
aws --profile saml iam list-role-policies --role-name ROLE_NAME
```

AMS에서 스택 IDs 찾기

스택 ID를 찾으려면 Amazon EC2 콘솔, AMS 콘솔 또는 AMS SKMS API/CLI를 사용할 수 있습니다.

AMS 콘솔:

- 탐색 창에서 RFCs 선택한 다음 스택을 생성한 RFC를 클릭합니다. 상단의 필터 옵션을 사용하여 목록을 줄입니다. RFC 세부 정보 페이지가 열리고 스택 ID와 함께 실행 출력이 포함됩니다.
- 또는 탐색 창에서 스택을 선택하여 스택 목록 페이지를 연 다음 스택 목록을 통해 원하는 스택으로 이동할 수 있습니다. 이 방법은 찾고 있는 스택의 주제를 알고 있는 경우에 더 유용합니다.

Amazon EC2 콘솔:

탐색 창에서 인스턴스 또는 로드 밸런서 또는 Auto Scaling 그룹을 선택합니다.

AMS SKMS API ListStackSummaries 또는 CLI:

Note

이러한 명령이 작동하려면 AMS CLI가 설치되어 있어야 합니다. AMS API 또는 CLI를 설치하려면 AMS 콘솔 개발자 리소스 페이지로 이동합니다. AMS CM API 또는 AMS SKMS API에 대한 참조 자료는 사용 설명서의 AMS 정보 리소스 섹션을 참조하세요. 인증 `--profile` 옵션을 추가해야 할 수 있습니다. 예: `aws amsskms ams-cli-command --profile SAML`.와 같이 모든 AMS 명령이 `us-east-1`에서 부족하므로 `--region` 옵션을 추가해야 할 수도 있습니다. `aws amscm ams-cli-command --region=us-east-1`.

Note

AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다. us-east-1. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 때 --region us-east-1 값을 추가해야 할 수 있습니다. 인증 방법인 --profile saml 경우를 추가해야 할 수도 있습니다.

현재 계정의 스택 목록을 보려면 SKMS API(CLI:)의 ListStackSummaries 작업을 실행합니다. list-stack-summaries. 특정 스택 인스턴스에 대한 전체 정보를 가져오려면 StackId에서 GetStack을 실행합니다.

- 다음 예제에서 첫 번째 명령은 계정의 모든 스택 인스턴스에 대한 요약 목록을 요청합니다. 두 번째 명령은 특정 스택 템플릿의 인스턴스만 나열하고 VpcId, 이름 및 StackId를 출력하기 위해 쿼리 필터와 함께 스택 인스턴스 목록을 요청합니다.

```
aws amsskms list-stack-summaries --output table
```

```
-----
|                               ListStackSummaries                               |
|                               StackSummaries                                |
+-----+-----+-----+-----+
| VpcId   | StackId   | StackTemplateId | Name   |
+-----+-----+-----+-----+
| vpc-0123abcd | stack-1fb7fe2212345678 | stm-sdhopvbb123456789 | Test ELB |
| vpc-0123abcd | stack-8323cc0e12345678 | stm-s2b72beb123456789 | S3 store |
| vpc-0123abcd | stack-2309fa0712345678 | stm-sdhopvbb123456789 | ELB      |
| vpc-0123abcd | stack-5e61a70512345678 | stm-sdpabqbb123456789 | PatchSim |
| vpc-0123abcd | stack-bd0e080d12345678 | stm-s2b72beb123456789 | CLI demo |
+-----+-----+-----+-----+
```

CLI 쿼리 사용에 대한 자세한 내용은 [--query 옵션을 사용하여 출력을 필터링하는 방법](#) 및 쿼리 언어 참조인 [JMESPath 사양](#)을 참조하세요.

Note

액세스에 인스턴스 IDs 사용하는 방법에 대한 자세한 내용은 단원을 참조하십시오 [Bastion을 사용하여 인스턴스에 액세스](#).

AMS에서 인스턴스 IDs 또는 IP 주소 찾기

- 인스턴스에 대한 액세스를 요청하거나, 인스턴스에 로그인하거나, AMI를 생성하려면 인스턴스 ID가 있어야 합니다. EC2 인스턴스(독립 실행형 인스턴스 또는 스택의 일부) 또는 데이터베이스 인스턴스의 경우 다음과 같은 몇 가지 방법으로 ID를 찾을 수 있습니다.
- ASG 스택의 인스턴스에 대한 AMS 콘솔: 스택을 생성한 RFC의 RFC 세부 정보 페이지를 확인합니다. 실행 출력 섹션에서 ASG 스택의 스택 ID를 찾은 다음 EC2 콘솔 Auto Scaling 그룹 페이지로 이동하여 해당 스택 ID를 검색하고 해당 스택에 대한 인스턴스를 찾을 수 있습니다. 인스턴스를 찾으면 인스턴스를 선택하면 페이지 하단에 IP 주소를 포함한 세부 정보가 포함된 영역이 열립니다.
- 독립 실행형 EC2 또는 데이터베이스(DB) 인스턴스용 AMS 콘솔: EC2 스택 또는 DB 인스턴스를 생성한 RFC의 RFC 세부 정보 페이지를 확인합니다. 실행 출력 섹션에서 인스턴스 ID 및 IP 주소를 찾을 수 있습니다.
- AWS EC2 콘솔:
 - 탐색 창에서 [인스턴스(Instances)]를 선택합니다. 인스턴스 페이지가 열립니다.
 - ID를 사용할 인스턴스를 클릭합니다. 인스턴스 세부 정보 페이지가 열리고 ID 및 IP 주소가 표시됩니다.
- AWS 데이터베이스 콘솔:
 - 홈 페이지에서 DB 인스턴스를 선택합니다. 인스턴스 페이지가 열립니다.
 - ID를 사용할 DB 인스턴스를 필터링합니다. 인스턴스 세부 정보 페이지가 열리고 ID가 표시됩니다.
- AMS CLI/API.

Note

이러한 명령이 작동하려면 AMS CLI가 설치되어 있어야 합니다. AMS API 또는 CLI를 설치하려면 AMS 콘솔 개발자 리소스 페이지로 이동합니다. AMS CM API 또는 AMS SKMS API에 대한 참조 자료는 사용 설명서의 AMS 정보 리소스 섹션을 참조하세요. 인증 --profile 옵션을 추가해야 할 수 있습니다. 예: `aws amsskms ams-cli-command --profile SAML`. 와 같이 모든 AMS 명령이 us-east-1에서 실행되므로 --region 옵션을 추가해야 할 수도 있습니다 `aws amscm ams-cli-command --region=us-east-1`.

 Note

AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다. us-east-1. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 때 --region us-east-1 값을 추가해야 할 수 있습니다. 인증 방법인 --profile sam1 경우를 추가해야 할 수도 있습니다.

다음 명령을 실행하여 스택 실행 출력 세부 정보를 가져옵니다.

```
aws amsskms get-stack --stack-id STACK_ID
```

출력은 하단 근처의 아래에 InstanceId가 나타나는 것과 비슷합니다 Outputs(표시된 값은 예제임).

```
{
  "Stack": {
    "StackId": "stack-7fa52bd5eb8240123",
    "Status": {
      "Id": "CreateCompleted",
      "Name": "CreateCompleted"
    },
    "VpcId": "vpc-01234567890abcdef",
    "Description": "Amazon",
    "Parameters": [
      {
        "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
        "Key": "SecurityGroups"
      },
      {
        "Value": "subnet-01234567890abcdef",
        "Key": "InstanceSubnetId"
      },
      {
        "Value": "t2.large",
        "Key": "InstanceType"
      },
      {
        "Value": "ami-01234567890abcdef",
```

```

        "Key": "InstanceAmiId"
      }
    ],
    "Tags": [],
    "Outputs": [
      {
        "Value": "i-0b22a22eec53b9321",
        "Key": "InstanceId"
      },
      {
        "Value": "10.0.5.000",
        "Key": "InstancePrivateIP"
      }
    ],
    "StackTemplateId": "stm-s6xvs0000000000000",
    "CreatedTime": "1486584508416",
    "Name": "Amazon"
  }
}

```

AMS에서 Amazon 리소스 이름(ARNs) 찾기

Amazon 리소스 이름(ARN)은 EC2 인스턴스, S3 버킷, 계정, Lambda 함수 등과 같은 AWS 리소스를 고유하게 식별하는 문자열입니다. IAM 정책 AWS, Amazon Relational Database Service(Amazon RDS) 태그, API 호출 등 모든에서 리소스를 명확하게 지정하려는 경우 ARN이 AWS 필요합니다. ARNs은 서비스, 리전, 계정 및 기타 정보를 지정하는 식별자로 구성됩니다. 세 가지 ARN 형식이 있습니다.

```

arn:aws:service:region:account-id:resource-id
arn:aws:service:region:account-id:resource-type/resource-id
arn:aws:service:region:account-id:resource-type:resource-id

```

Note

ARN의 정확한 형식은 서비스 및 리소스 유형에 따라 달라집니다. ARN에 대한 자세한 내용은 [Amazon 리소스 이름\(ARNs\)과 AWS 서비스 네임스페이스](#) 및 [ARN 형식을 참조하세요](#). 리소스별 ARN 형식 예제는 AWS 서비스 권한 부여 참조 [리소스 유형 테이블](#)을 참조하세요.

AWS 객체의 ARN을 찾는 것은 어려울 수 있습니다. 시도하는 세 가지 방법은 다음과 같습니다.

- AWS 서비스 콘솔: 관련 AWS 서비스 콘솔로 이동하여 리소스를 찾고 리소스 세부 정보에서 ARN을 찾습니다.
- AWS API/CLI(먼저 AWS CLI를 설치해야 함): [AWS CLI 명령 참조](#)에서 관련 서비스를 찾은 다음 AWS 서비스에 따라 describe, 또는 등과 같은 관련 작업을 찾습니다.get. 예를 들어 모든 IAM 역할, 정책 및 사용자에 대해 다음을 사용하여 CLI의 출력에서 ARN을 가져올 수 있습니다.

```
aws iam get-role --role-name EMR_DefaultRole
```

- 관련 형식을 기반으로 ARN 구성: [AWS 서비스의 작업, 리소스 및 조건 키](#)를 살펴보고 관련 서비스를 찾은 다음 관련 작업을 찾은 다음 리소스 ARN 형식으로 드릴다운하여 리소스의 ARN 형식을 찾습니다. 형식이 지정되면 변수를 관련 설정으로 바꿉니다.

적절한 형식(서비스 및 리소스 유형에 따라 형식 변경)을 따르고 정보를 입력하여 ARN을 직접 구성할 수 있습니다. 다음은 몇 가지 ARN 예제입니다.

- AWS 계정 ARN의 구문은 다음과 같습니다.

```
arn:aws:iam::ACCOUNT-ID:root
```

- S3 ARN에는 버킷 및 관련 객체의 플랫폼 계층 구조가 있습니다.

```
arn:aws:s3:::ams-bucket
```

- EC2 ARN에는 이미지, 보안 그룹, 인스턴스 등과 같은 하위 리소스 유형이 있습니다. 이 예제는 끝에 인스턴스 ID를 포함합니다.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-012abcd34efghi56
```

- Lambda ARN에는 resource-id 파트의 함수 이름이 있으며,이 예제와 같이 끝에 버전 번호를 포함해야 할 수 있습니다.

```
arn:aws:lambda:us-east-1:123456789012:function:api-function:1
```

AWS Key Management Service 서비스는 키 [ID 및 키 ARN 찾기](#) 정보를 제공합니다.

DynamoDB 테이블의 ARN을 찾으려면 DynamoDB [describe-table](#) CLI를 사용합니다.

외부자의 AWS ARNs 살펴보기는 [AWS ARN Explained: Amazon Resource Name Guide](#)를 참조하세요.

AMS에서 ARN으로 리소스 찾기

Amazon 리소스 이름(ARNs) AWS 리소스를 고유하게 식별합니다. ARN 및 ARN 형식에 대한 자세한 내용은 [Amazon 리소스 이름\(ARNs\) 및 AWS 서비스 네임스페이스](#) 및 [ARN 형식을 참조하세요](#).

Note

ARN에서 리소스에 대한 세부 정보를 얻으려면 리소스를 생성한 계정에 액세스할 수 있어야 합니다.

서비스에는 다양한 관련 정보가 있는 여러 리소스 유형이 있기 때문에 어느 리소스 ARN에서 모든 리소스 세부 정보를 조회 AWS 할 수 있는 직접 경로가 없습니다. 리소스에 대한 ARN이 있는 경우 다음을 확인할 수 있습니다.

- 관련 AWS 서비스(세 번째 ARN 세그먼트)는 리소스를 찾기 위해 살펴볼 AWS 콘솔을 알려줍니다.
- 리소스 ID(6번째 또는 7번째 ARN 세그먼트)는 올바른 리소스를 찾았음을 확인합니다.

또는 AWS CLI 명령 참조에서 [AWS 해당 서비스에 사용할 수 있는 CLI 명령을](#) 찾아 리소스에 대한 세부 정보를 얻을 수 있습니다.

예를 들어 다음 ARN에서 서비스가 이고, lambda계정이 이고123456789012, 리소스 유형이 이고function, 함수 이름이 임을 확인할 수 있습니다TestFunction.

```
arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

여기에서 [AWS Lambda 서비스에 대한 CLI 설명서를](#) 검토하여 get-function 및와 같은 다양한 명령으로 추가 세부 정보를 검색하는 방법을 알아볼 수 있습니다get-function-configuration.

예를 들어 이름이나 ARN이 있는 경우 다음 명령을 사용하여 Lambda 함수에 대한 자세한 정보를 가져올 수 있습니다.

```
aws lambda get-function-configuration --function-name TestFunction
```

```
aws lambda get-function-configuration --function-name arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

AMS 계정 설정 찾기

AMS RFCs, 일정을 설정하고, 알림을 받는 사용자를 결정하는 데 사용되는 계정 설정입니다.

일부 설정은 온보딩 중에 생성되며 서비스 요청을 변경해야 합니다. AMS와 통신할 때 사용할 것이므로 이러한 계정 세부 정보를 기록해 두어야 합니다.

- **자격 증명:** AMS 사용자 이름 또는 암호를 검색해야 하는 경우 로컬 IT 관리자에게 문의하세요. AMS는 회사 Active Directory를 사용합니다.
- **Cloud Service Delivery Manager(CSDM):** 이 사용자는 AMS와의 연락 담당자이며 서비스 질문에 답변할 수 있습니다. 온보딩 시이 사람의 연락처 정보가 제공되므로 AMS와 상호 작용하는 조직의 모든 사용자가 해당 정보를 사용할 수 있도록 유지해야 합니다. 이 사용자로부터 AMS 서비스에 대한 월별 보고서를 받을 수 있습니다.
- **콘솔 액세스:** 계정에 대해 특별히 설정된 URL로 AMS 콘솔에 액세스합니다. CSDM에서 URL을 가져올 수 있습니다.
- **AMS CLI:** AMS 콘솔 개발자의 리소스 페이지 또는 CSDM에서 가져오는 배포 가능 패키지를 통해 AMS CLI를 가져올 수 있습니다. 배포 가능 패키지가 있으면 [AMS CLI 설치 또는 업그레이드](#)에 설명된 단계를 따릅니다.
- **유지 관리 기간:** 유지 관리 기간에 따라 EC2 인스턴스에 대한 패치 적용 시기가 결정됩니다. AWS Managed Services 유지 관리 기간(또는 유지 관리 기간)은 AWS Managed Services(AMS)에 대한 유지 관리 활동을 수행하고 태평양 표준시 기준 매월 두 번째 목요일 오후 3시부터 오후 4시까지 반복됩니다. AMS는 48시간 전에 통지하여 유지 관리 기간을 변경할 수 있습니다. 온보딩 시 다른 기간을 선택했을 수 있습니다. 선택한 유지 관리 기간의 레코드를 보관합니다.
- **모니터링:** AMS는 기본적으로 CloudWatch 지표 세트를 제공하지만 추가 지표를 요청할 수도 있습니다. 그렇다면 기록해 둡니다.
- **로그:** 기본적으로 로그는 `ams-a-ACCOUNT_ID-log-management-REGION`에 저장됩니다. 여기서 **REGION**은 로그가 생성된 리전입니다.
- **완화:** 온보딩 시 AMS는 리소스에 대한 맬웨어 공격이 식별되는 경우 선택한 완화 조치를 기록합니다. 예를 들어 특정 사용자에게 문의합니다. AMS와 상호 작용하는 조직의 모든 사용자가이 정보를 사용할 수 있도록 합니다.
- **리전:** AMS 콘솔에서 VPC 세부 정보 페이지를 볼 수 있습니다. AMS SKMS CLI를 설치한 후이 명령을 실행할 수도 있습니다(이 명령은 SAML 프로파일을 사용하며 인증 방법이 다른 경우 제거).

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

⚠ Important**i Note**

AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다. us-east-1. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 --region us-east-1 때를 추가해야 할 수 있습니다. 인증 방법인 --profile sam1 경우를 추가해야 할 수도 있습니다.

AMS에서 FQDNs 찾기

AWS Managed Services(AMS) 액세스 변경 유형(CTs)에는 AMS 신뢰 도메인의 정규화된 도메인 이름 또는 FQDN이 형식으로 필요합니다. C844273800838.amazonaws.com. AWS FQDN을 검색하려면 다음 중 하나를 수행합니다.

- AWS 콘솔: AWS Directory Service 콘솔의 디렉터리 이름 열을 살펴봅니다.
- CLI: 도메인에 로그인한 상태에서 다음 명령을 사용합니다.

Windows(사용자 및 FQDN 반환):

```
whoami /upn
```

또는 (DC+DC+DC=FQDN)

```
whoami /fqdn
```

Linux:

```
hostname --fqdn
```

i Note

AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다. us-east-1. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 --

`region us-east-1` 때를 추가해야 할 수 있습니다. 인증 방법인 `--profile saml` 경우를 추가해야 할 수도 있습니다.

AMS에서 가용 영역(AZs) 찾기

가용 영역: 모든 계정에 가용 영역이 두 개 이상 있습니다. 가용 영역 이름을 정확하게 찾으려면 먼저 연결된 서브넷 ID를 알아야 합니다.

- AMS 콘솔: 탐색 창에서 VPCs 클릭한 다음 필요한 경우 관련 VPC를 클릭합니다. VPCs 세부 정보 페이지에서 서브넷 테이블의 관련 서브넷을 선택하여 연결된 가용 영역의 이름이 있는 서브넷 세부 정보 페이지를 엽니다.
- AMS SKMS API/CLI:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

Note

AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다. `us-east-1`. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 `--region us-east-1` 때를 추가해야 할 수 있습니다. 인증 방법인 `--profile saml` 경우를 추가해야 할 수도 있습니다.

AMS에서 SNS 주제 찾기

SNS 주제에 따라 다양한 상황에서 알림을 받는 사람이 결정됩니다. AMS는 AMI 알림([SNS를 사용한 AMS AMI 알림 참조](#)), CloudWatch 경보 및 EC2 리소스([AMS에서 생성한 알림 수신 참조](#)) 등에 대한 SNS 주제를 제공합니다. CloudWatch EC2 <https://docs.aws.amazon.com/managedservices/latest/userguide/sent-alert-views.html> 기존 SNS 주제를 검색하려면:

- AWS 콘솔: SNS 콘솔을 사용하여 모든 주제, 애플리케이션 및 구독과 메시지 그래프를 볼 수 있습니다. 또한 주제를 생성, 삭제, 구독 및 게시합니다.
- API/CLI(AMS 계정에 로그인한 경우 AWS CLI 필요):

SNS 주제를 나열합니다.

```
aws sns list-topics
```

SNS 구독을 나열합니다.

```
aws sns list-subscriptions
```

Note

AMS API/CLI(amscm 및 amsskms) 엔드포인트는 AWS 버지니아 북부 리전에 있습니다us-east-1. 인증 설정 방식과 계정 및 리소스가 있는 AWS 리전에 따라 명령을 실행할 --region us-east-1 때를 추가해야 할 수 있습니다. 인증 방법인 --profile saml 경우를 추가해야 할 수도 있습니다.

AMS에서 백업 설정 찾기

백업 및 스냅샷은 네이티브 [AWS Backup](#) 서비스를 통해 AMS에서 관리합니다.

구성은 AWS Backup 계획을 통해 관리됩니다. 태그가 지정된 리소스를 백업 일정 및 보존 정책과 연결하는 여러 AWS Backup 계획이 있을 수 있습니다. AMS 계정 AWS Backup 설정을 찾으려면 <https://console.aws.amazon.com/backup> 콘솔 또는 [백업](#) 명령에 대한 AWS CLI 명령 참조를 사용합니다.

AMS 및에 대한 자세한 내용은 연속성 관리를 AWS Backup참조하세요. <https://docs.aws.amazon.com/managedservices/latest/userguide/continuity-mgmt.html>

AMS의 액세스 관리

SSH 또는 RDP(원격 데스크톱 프로토콜)를 사용하여 리소스에 액세스하는 방법과 Bastion을 사용하는 방법을 알아봅니다.

AWS Managed Services(AMS) 액세스 관리 시스템은 온보딩 중에 구성됩니다. AMS를 통해 페더레이션된 AMS IAM 사용자 역할을 가진 사용자만 계정의 AMS 리소스에 액세스할 수 있습니다.

다음에 설명된 연합 신뢰 외에도 AMS 보안 그룹은 프라이빗 및 퍼블릭 애플리케이션 액세스에서 중요한 요소입니다. AMS 보안 그룹 및 변경 방법에 대한 자세한 내용은 섹션을 참조하세요 [보안 그룹](#).

주제

- [액세스 관리란 무엇입니까?](#)
- [AMS에서 루트 사용자 계정을 사용하는 방법 및 시기](#)
- [AMS Advanced 콘솔 및 Amazon EC2 액세스](#)
- [AWS 관리 콘솔 및 AMS 콘솔 액세스](#)
- [Bastion을 사용하여 인스턴스에 액세스](#)

액세스 관리란 무엇입니까?

액세스 관리는 AMS가 승인되고 인증된 액세스만 허용하여 리소스를 보호하는 방법입니다. AMS는 기본 IAM 사용자 역할 및 인스턴스 프로파일과 다중 인증, 보안 그룹, DNS 친화적인 접속 이름 등을 사용하여 리소스를 보호합니다.

AMS는 관리가 필요한 세 가지 유형의 액세스에 중점을 둡니다.

- 콘솔 액세스: 계정의 Active Directory에 있는 사용자는 연동을 활용하여 SSO(Single Sign-On)를 사용하여 콘솔에 액세스할 수 있습니다. 이러한 계정에 대해 다중 인증이 구성된 경우 MFA가 콘솔에 액세스하도록 계속 요구할 수 있습니다.
- RDP 또는 SSH를 사용한 인스턴스 액세스: Active Directory 신뢰를 활용하여 계정의 기존 Active Directory 사용자는 인스턴스에 대한 액세스를 요청한 다음 기존 기업 자격 증명을 사용하여 접속 및 인스턴스에 성공적으로 인증할 수 있습니다. 이러한 계정에 대해 다중 인증이 구성된 경우 MFA가 인스턴스에 대한 액세스를 요청하도록 계속 요구할 수 있습니다. AMS는 자체 MFA 솔루션을 사용하여 인스턴스에 대한 AMS 엔지니어 액세스를 제한합니다.
- 애플리케이션 액세스: 사용 사례에 따라 다릅니다.

주제

- [AMS가 계정에 액세스하는 이유와 시간](#)

AMS가 계정에 액세스하는 이유와 시간

AWS Managed Services(AMS)는 AWS 인프라를 관리하며, 특정 이유로 AMS 운영자와 관리자가 계정에 액세스하는 경우도 있습니다. 이러한 액세스 이벤트는 AWS CloudTrail (CloudTrail) 로그에 문서화됩니다.

AMS가 계정에 액세스하는 이유, 시기 및 방법은 다음 주제에 설명되어 있습니다.

AMS 고객 계정 액세스 트리거

AMS 고객 계정 액세스 활동은 트리거에 의해 구동됩니다. 오늘 트리거는 Amazon CloudWatch(CloudWatch) 경보 및 이벤트에 대한 응답으로 문제 관리 시스템에서 생성된 AWS 티켓과 제출한 인시던트 보고서 또는 서비스 요청입니다. 각 액세스에 대해 여러 서비스 호출 및 호스트 수준 활동을 수행할 수 있습니다.

액세스 근거, 트리거 및 트리거의 이니시에이터는 다음 표에 나열되어 있습니다.

액세스 트리거

액세스	시작한 사용자	트리거
패치 적용	AMS	패치 문제
인프라 배포	AMS	배포 문제
내부 문제 조사	AMS	문제 문제(시스템적으로 식별된 문제)
알림 조사 및 문제 해결	AMS	AWS Systems Manager 운영 작업 항목(SSM OpsItems)
수동 RFC 실행	사용자	변경 요청(RFC) 문제입니다. (자동화되지 않은 RFCs 리소스에 대한 AMS 액세스가 필요할 수 있음)

액세스	시작한 사용자	트리거
인시던트 조사 및 해결	사용자	인바운드 지원 사례(제출한 인시던트 또는 서비스 요청)
인바운드 서비스 요청 이행	사용자	

AMS 고객 계정 액세스 IAM 역할

트리거되면 AMS는 AWS Identity and Access Management (IAM) 역할을 사용하여 고객 계정에 액세스합니다. 계정의 모든 활동과 마찬가지로 역할 및 사용량은 CloudTrail에 기록됩니다.

 Important

이러한 역할을 수정하거나 삭제하지 마십시오.

고객 계정에 대한 AMS 액세스를 위한 IAM 역할

역할 이름	계정 유형(SALZ, MALZ 관리, MALZ 애플리케이션 등)	설명
ams-service-admin	SALZ, MALZ	패치, 백업, 자동 문제 해결과 같은 AMS 서비스 자동화 액세스 및 자동 인프라 배포.
ams-application-infra-read-only	SALZ, MALZ 애플리케이션, MALZ 도구-애플리케이션	운영자 읽기 전용 액세스
ams-application-infra-operations		인시던트/서비스 요청에 대한 운영자 액세스
ams-application-infra-admin		AD 관리자 액세스
ams-primary-read-only	MALZ 관리	운영자 읽기 전용 액세스
ams-primary-operations		인시던트/서비스 요청에 대한 운영자 액세스

역할 이름	계정 유형(SALZ, MALZ 관리, MALZ 애플리케이션 등)	설명
ams-primary-admin		AD 관리자 액세스
ams-logging-read-only		운영자 읽기 전용 액세스
ams-logging-operations	MALZ 로깅	인시던트/서비스 요청에 대한 운영자 액세스
ams-logging-admin		AD 관리자 액세스
ams-networking-read-only		운영자 읽기 전용 액세스
ams-networking-operations	MALZ 네트워킹	인시던트/서비스 요청에 대한 운영자 액세스
ams-networking-admin		AD 관리자 액세스
ams-shared-services-read-only		운영자 읽기 전용 액세스
ams-shared-services-operations	MALZ 공유 서비스	인시던트/서비스 요청에 대한 운영자 액세스
ams-shared-services-admin		AD 관리자 액세스
ams-security-read-only		운영자 읽기 전용 액세스
ams-security-operations	MALZ 보안	인시던트/서비스 요청에 대한 운영자 액세스
ams-security-admin		AD 관리자 액세스
ams-access-security-analyst	SALZ, MALZ 애플리케이션, MALZ 도구-애플리케이션, MALZ Core	AMS 보안 액세스
ams-access-security-analyst-read-only		AMS 보안, 읽기 전용 액세스

역할 이름	계정 유형(SALZ, MALZ 관리, MALZ 애플리케이션 등)	설명
Sentinel_AdminUser_Role_PXHazRQadu0PVcCDcMbHE	SALZ	[BreakGlassRole]breakGlass를 고객 계정으로 나누는 데 사용됩니다.
Sentinel_PowerUser_Role_wZuPuS0ROOI0lazDbRI9		RFC 실행을 위한 고객 계정에 대한 Poweruser 액세스
Sentinel_ReadOnlyUser_Role_Pd4L6Rw9RD0InLkD5JOo		RFC 실행을 위한 고객 계정에 대한 ReadOnly 액세스
ams_admin_역할	SALZ, MALZ	RFC 실행을 위한 고객 계정에 대한 관리자 액세스
AWSManagedServices_Provisioning_CustomerStacksRole		CloudFormation Ingest를 통해 고객을 대신하여 CFN 스택을 시작하고 업데이트하는 데 사용됩니다.
customer_ssm_automation_역할		실행서 실행을 위해 CT 실행에 의해 SSM Automation으로 전달되는 역할
ams_ssm_automation_역할	SALZ, MALZ 애플리케이션, MALZ Core	실행서 실행을 위해 AMS 서비스가 SSM Automation에 전달하는 역할
ams_ssm_iam_deployment_역할	MALZ 애플리케이션	IAM 카탈로그에서 사용하는 역할
ams_ssm_shared_services_intermediary_role	MALZ 공유 서비스	애플리케이션 ams_ssm_automation_role이 공유 서비스 계정에서 특정 SSM 문서를 실행하는 데 사용하는 역할

역할 이름	계정 유형(SALZ, MALZ 관리, MALZ 애플리케이션 등)	설명
AmsOpsCenterRole		고객 계정에서 OpsItems 생성하고 업데이트하는 데 사용됩니다.
AMSOpsItemAutoExecutionRole	SALZ, MALZ	SSM 문서를 가져오고, 리소스 태그를 설명하고, OpsItems 업데이트하고, 자동화를 시작하는 데 사용됩니다.
customer-mc-ec2-instance-profile		기본 고객 EC2 인스턴스 프로파일(역할)

인스턴스 액세스 요청

리소스에 액세스하려면 먼저 해당 액세스에 대한 변경 요청(RFC)을 제출해야 합니다. 요청할 수 있는 액세스에는 관리자(읽기/쓰기 권한)와 읽기 전용(표준 사용자 액세스)의 두 가지 유형이 있습니다. 액세스는 기본적으로 8시간 동안 지속됩니다. 이 정보는 필수입니다.

- 액세스하려는 인스턴스의 스택 ID 또는 스택 IDs.
- AMS 신뢰 도메인의 정규화된 도메인 이름입니다.
- 액세스하려는 사람의 Active Directory 사용자 이름입니다.
- 스택이 액세스하려는 VPC의 ID입니다.

액세스 권한이 부여되면 필요에 따라 요청을 업데이트할 수 있습니다.

액세스를 요청하는 방법의 예는 [스택 관리자 액세스 | 권한 부여](#) 또는 [스택 읽기 전용 액세스 | 권한 부여](#)를 참조하세요.

AMS에서 루트 사용자 계정을 사용하는 방법 및 시기

[루트 사용자](#)는 계정 AWS 내의 슈퍼유저입니다. AMS는 루트 사용량을 모니터링합니다. 계정 설정 변경, 결제 및 비용 관리에 대한 (IAM) 액세스 활성화 AWS Identity and Access Management, 루트 암호 변경, 멀티 팩터 인증(MFA) 활성화 등 필요한 몇 가지 작업에만 루트를 사용하는 것이 좋습니다. AWS Identity and Access Management 사용 설명서의 [루트 사용자 자격 증명이 필요한 작업을 참조하세요](#).

Note

MFA는 특히 루트 사용자 액세스를 허용하지 않도록 AMS Advanced 온보딩 중에 활성화됩니다. AMS 관리형 계정의 루트 액세스는 다른 AWS 계정과 다르며 전체 AMS 관리형 환경의 보안에 매우 중요합니다. 구성된 MFA는 가상 MFA이며 AMS 소유 디바이스를 사용하여 수행됩니다. AMS의 지원을 받아 가상 MFA를 구성하면 가상 토큰이 즉시 삭제됩니다. 이렇게 하면 사용자와 AMS 모두 루트 사용자로 계정에 로그인할 수 없습니다. 루트 로그인은 특별 요청(다음 설명)에서만 다시 활성화할 수 있으며 AMS는 이러한 액세스가 절대적으로 필요한 경우에만 사용될 것으로 예상합니다. MFA에 대한 자세한 내용은 [다중 인증으로 새 계정 보안을 참조하세요](#).

루트 액세스는 항상 AMS 보안 및 운영 팀 응답을 트리거합니다. AMS는 API 호출에서 루트 액세스를 모니터링하고 이러한 액세스가 감지되면 경보가 트리거됩니다.

루트 액세스 요청은 AMS 계정 유형 간에 약간 다릅니다.

AMS Advanced 단일 계정 랜딩 존을 사용한 루트 액세스:

단일 계정 랜딩 존이 있는 경우 클라우드 서비스 제공 관리자(CSDM) 및 클라우드 아키텍트(CAs)에게 문의하여 필요한 루트 액세스 작업에 대해 알립니다. 제안된 활동 전에 24시간 전에 알리는 것이 가장 좋습니다.

AMS Advanced 다중 계정 랜딩 존을 사용한 루트 액세스:

다중 계정 랜딩 존 애플리케이션, 공유 서비스, 보안 또는 네트워킹 계정의 경우 관리 | 기타 | 기타(ct-1e1xtak34nx76) 변경 유형을 사용합니다. 루트 사용자 자격 증명을 사용하는 날짜, 시간 및 목적을 포함하고 제안된 활동 전에 24시간 전에 알림을 제공하도록 RFC를 예약합니다. 다중 계정 랜딩 존 관리 계정을 사용하여 RFC를 제출합니다.

또한 24시간 전에 CSDM 및 CAs에 문의하여 필요한 루트 액세스 작업에 대해 알립니다.

AMS 작업 및 루트 사용에 대한 보안 응답:

AMS는 루트 사용자 계정이 사용될 때 경보를 수신합니다. 루트 자격 증명 사용이 예약되지 않은 경우 AMS 보안 팀 및 계정 팀에 문의하여 예상되는 활동인지 확인합니다. 예기치 않은 활동인 경우 AMS는 보안 팀과 협력하여 문제를 조사합니다.

AMS Advanced 콘솔 및 Amazon EC2 액세스

AMS Advanced 콘솔에 액세스.

Amazon EC2 인스턴스에 액세스.

액세스 요청 제출:

AMS Amazon EC2 인스턴스에 로그인:

AWS 관리 콘솔 및 AMS 콘솔 액세스

온보딩 중에 AWS 관리 콘솔에 대한 로그인이 제공됩니다(제한된 권한: AMS 콘솔에 쓸 수 있음, 고객 정보 페이지의 일부 필드). AWS 관리 콘솔에서 관리형 서비스 링크를 선택하여 AMS 콘솔에 액세스할 수 있습니다. 페더레이션 액세스 또는 공유 자격 증명(사용자 이름/암호)은 IT 관리 팀과 합의한 대로 준비됩니다. 계정 또는 그룹을 추가로 생성하려면 AMS에 서비스 요청을 제출합니다.

AWS 관리 콘솔에 액세스하는 방법에 대한 자세한 내용은 [AWS 관리 콘솔 작업을 참조하세요](#).

AMS 콘솔 사용에 대한 몇 가지 팁은 [AMS 콘솔 사용을 참조하세요](#).

임시 AMS 콘솔 액세스

AMS에 인증하도록 자격 증명 공급자(예: SAML)를 아직 설정하지 않은 경우 AMS 콘솔에 임시로 액세스할 수 있습니다. CSDM에 문의하여 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 엔터티 또는 정책 변경 요청 생성(ct-3dpd8mdd9jn1r)을 다음 값으로 제출합니다.

- Username: 생성 중인 IAM 사용자 엔터티의 이름입니다.
- AccessType: "콘솔 액세스"
- UserPermissions: "**USERNAME**(임시 액세스 권한을 부여하려는 사람)에 대한 임시 AMS 콘솔 액세스"
- 이메일 알림: 이메일 주소로, AMS가 요청할 때 요청을 승인할 수 있습니다.

Note

임시 AMS 콘솔 액세스를 위한 RFC는 내부 보안 팀과 AMS Global Security의 보안 검토 및 수락이 필요합니다.

이 요청이 완료되고 로그인할 수 있게 되면 생성된 RFC를 승인하여 승인을 추적하고 AMS 팀이 작업을 종료하도록 허용해야 합니다. RFC를 승인하려면 RFC의 목록 페이지에서 해당 RFC를 찾고(옆에 승인 보류 중 플래그가 있음) 해당 RFC의 RFC 세부 정보 페이지를 연 다음 승인을 선택합니다. RFC가 승인될 때까지 AMS를 사용할 수 없습니다.

RFC가 성공적으로 완료되면 AMS 작업은 새 IAM 사용자와 암호를 제공합니다. 그런 다음 다음 단계를 따릅니다.

1. AWS 관리 콘솔로 이동하여 제공된 자격 증명으로 로그인합니다. 새 암호를 생성하라는 메시지가 표시됩니다. 또한 로그인 시 다중 인증(MFA)을 설정해야 합니다. 이에 대한 자세한 내용은 [에서 Multi-Factor Authentication \(MFA\) 사용을 AWS](#) 참조하세요.
2. AWS 관리 콘솔에서 제공된 IAM 역할()로 변경합니다
다customer_ *CustomerCode* _readonly_user_role.
3. AMS Managed Services 콘솔을 엽니다.

Note

임시 액세스의 기본값은 60일이지만 CSDM에 문의하여 30일 연장을 요청할 수 있습니다.

Bastion을 사용하여 인스턴스에 액세스

고객과 AMS 운영자 모두 AMS 관리형 계정 내의 리소스에 대한 모든 액세스는 접속 호스트를 사용하여 게이트됩니다. 다중 계정 랜딩 존(MALZ) 및 단일 계정 랜딩 존(SALZ) AMS Advanced 계정 모두에 대한 액세스를 위해 Linux 및 Windows RDP 접속을 모두 유지합니다.

접속은 프라이빗 연결(VPN 또는 AWS Direct Connect)DX를 통해서만 액세스할 수 있습니다. 인바운드 트래픽을 방지하기 위한 방화벽 외에도 접속은 고정된 일정에 따라 정기적으로 재프로비저닝됩니다(기존 자격 증명 사용).

Note

파일을 EC2 인스턴스로 이동하는 방법에 대한 자세한 내용은 [파일 전송: 로컬 Windows 또는 MAC PC를 Linux Amazon EC2로](#) 참조하세요.

MALZ

Active Directory(AD) 자격 증명으로 접속 인스턴스에 로그인하여 계정 인스턴스에 액세스합니다. Amazon은 경계 네트워크 VPC(네트워킹 계정)에 있는 접속을 사용하며, 공유 서비스 계정의 Customer Bastions 서브넷에 있는 고객 접속을 사용합니다.

AMS 환경이 처음 온보딩되면 선택에 따라 SSH 접속 2개와 RDP 접속 2개가 생깁니다.

SALZ

Active Directory(AD) 자격 증명으로 접속 인스턴스에 로그인하여 계정 인스턴스에 액세스합니다. AMS는 경계 네트워크 서브넷에 있는 접속을 사용하며 프라이빗 서브넷에 있는 접속을 사용합니다.

계정이 처음 온보딩되면 기본적으로 두 개의 RDP와 두 개의 SSH 접속이 있습니다.

Note

단일 계정 랜딩 존의 일부로 AMS는 스택에 액세스할 수 있는 RDP(Windows) 및 SSH(Linux) Bastion을 모두 제공하지만 RDP Bastion만 사용할지 SSH Bastion만 사용할지 선택할 수 있습니다. RDP만 또는 SSH 접속만 유지되도록 요청하려면 서비스 요청을 제출합니다.

인스턴스에 액세스하려면 다음이 필요합니다.

- 스택에 부여된 액세스 권한입니다. 스택에 대한 액세스 권한을 얻으려면 [스택 관리자 액세스 권한 | 권한 부여](#) 또는 [스택 읽기 전용 액세스 권한 | 권한 부여](#)를 참조하세요.
- 인스턴스에 대한 액세스 권한을 부여받을 수 있도록 액세스하려는 스택 ID입니다. 스택 ID를 찾으려면 섹션을 참조하세요 [AMS에서 스택 IDs 찾기](#).
- 액세스하려는 인스턴스 IP입니다. 인스턴스 IP를 찾으려면 섹션을 참조하세요 [AMS에서 인스턴스 IDs 또는 IP 주소 찾기](#).
- DNS 친화적인 접속 이름 또는 접속 IP입니다. DNS 친화적인 접속 이름을 사용하는 방법과 접속 IP를 찾는 방법은 다음에 설명되어 있습니다.

DNS 친화적인 접속 이름

AWS Managed Services(AMS)는 DNS 친화적인 접속 이름을 사용합니다.

MALZ

다중 계정 랜딩 존(MALZ)의 경우 AMS 관리형 Active Directory의 FQDN에 있는 접속에 대한 DNS 레코드가 생성됩니다. AMS는 필요에 따라 Linux 및 Windows 접속을 대체합니다. 예를 들어 배포해야 하는 새 접속 AMI가 있는 경우 접속 DNS 레코드는 새롭고 유효한 접속을 가리키도록 동적으로 업데이트됩니다.

1. SSH(Linux) 접속에 액세스하려면 다음과 같은 DNS 레코드를 사용합니다.

`sshbastion(1-4).Your_Domain.com`

예를 들어 도메인이 인 경우Your_Domain:

- `sshbastion1.Your_Domain.com`
- `sshbastion2.Your_Domain.com`
- `sshbastion3.Your_Domain.com`
- `sshbastion4.Your_Domain.com`

2. RDP(Windows) 접속에 액세스하려면 다음과 같은 DNS 레코드를 사용합니

`다rdp-Username.Your_Domain.com`.

예를 들어 사용자 이름이 , alex, demo또는 test이고 도메인이 bob인 경우Your_Domain.com:

- `rdp-alex.Your_Domain.com`
- `rdp-test.Your_Domain.com`
- `rdp-demo.Your_Domain.com`
- `rdp-bob.Your_Domain.com`

SALZ

단일 계정 랜딩 존(SALZ)은 필요에 따라 Linux 및 Windows 접속을 대체합니다. 예를 들어 배포해야 하는 새 접속 AMI가 있는 경우 접속 DNS 레코드는 새롭고 유효한 접속을 가리키도록 동적으로 업데이트됩니다.

1. SSH(Linux) 접속에 액세스하려면 다음과 같은 DNS 레코드를 사용합니다.

`sshbastion(1-4).AAccountNumber.amazonaws.com`.

예를 들어, 여기서 123456789012는 계정 번호입니다.

- sshbastion1.A123456789012.amazonaws.com
- sshbastion2.A123456789012.amazonaws.com
- sshbastion3.A123456789012.amazonaws.com
- sshbastion4.A123456789012.amazonaws.com

2. RDP(Windows) 접속에 액세스하려면 다음과 같은 DNS 레코드를 사용합니다.
drrdpbastion(1-4).ACCOUNT_NUMBER.amazonaws.com.

예를 들어, 여기서 123456789012는 계정 번호입니다.

- rdpbastion1.A123456789012.amazonaws.com
- rdpbastion2.A123456789012.amazonaws.com
- rdpbastion3.A123456789012.amazonaws.com
- rdpbastion4.A123456789012.amazonaws.com

단일 계정 랜딩 존(SALZ) 접속 비용 절감

AMS는 Amazon EC2 인스턴스에 연결할 수 있도록 기본 구성에서 SSH 접속 2개와 RDP 접속 2개를 제공하며 서비스 작업을 위한 기본 구성에서 DMZ 접속 2개를 배포합니다. Bastion은 기본적으로 m4. 대규모 Amazon EC2 인스턴스를 사용합니다. Bastion에 사용되는 Amazon EC2 인스턴스를 t3.small로 변경하고 비용을 절감할 수 있습니다.

온디맨드 인스턴스, 스팟 인스턴스 또는 절감형 풀렌을 사용하는 경우이 기능을 고려하고 비용을 절감해야 합니다. 예약 인스턴스를 사용하는 경우 t3.small 인스턴스를 사용하면 비용이 절감될 수 있는지 고려합니다. 인스턴스 유형을 변경하려면 AMS 계정에서 관리 | 고급 스택 구성 요소 | EC2 인스턴스 스택 | 크기 조정(ct-15mazj88xc69) CT를 사용하여 RFC를 제출합니다.

추가 질문이 있거나이 기능을 활용할 수 있는지 확인하려면 클라우드 서비스 제공 관리자(CSDM)에게 문의하십시오.

접속 IP 주소 사용

AMS 고객은 앞서 [DNS 친화적인 접속 이름](#) 설명한 SSH 및 RDP 접속 또는 접속 IP 주소를 사용할 수 있습니다.

계정의 접속 IP 주소, SSH 및 RDP를 찾으려면:

1. 다중 계정 랜딩 존만 해당: 공유 서비스 계정에 로그인합니다.

2. EC2 콘솔을 열고 인스턴스 실행을 선택합니다.

인스턴스 페이지가 열립니다.

3. 상단의 필터 상자에 ssh-bastion 또는 rdp-bastion을 입력합니다.

상단의 필터 상자에 customer-ssh 또는 customer-rdp를 입력합니다.

계정의 SSH 및/또는 RDP 접속이 표시됩니다.

SSH 배스천 외에도 목록에 AMS 경계 네트워크 배스천이 표시될 수 있으며,이 배스천은 사용할 수 없습니다.

4. SSH 또는 RDP 접속을 선택합니다. Windows 컴퓨터를 사용하고 Linux 인스턴스에 로그인하려는 경우 SSH 접속을 사용합니다. Windows 인스턴스에 로그인하려면 RDP 접속을 사용합니다. Linux OS를 사용 중이고 Windows 인스턴스에 로그인하려는 경우 RDP 터널을 통해 SSH 접속을 사용합니다(Windows 데스크톱에 액세스할 수 있도록). Linux OS에서 Linux 인스턴스에 액세스하려면 SSH 접속을 사용합니다.

AMS의 인스턴스 액세스 예제

이 예제에서는 RFC를 통해 액세스 권한을 부여받은 후 Bastion을 사용하여 AMS 계정의 인스턴스에 로그인하는 방법을 보여줍니다. 액세스 권한 부여에 대한 자세한 내용은 섹션을 참조하세요 [인스턴스 액세스 요청](#).

Note

파일을 EC2 인스턴스로 이동하는 방법에 대한 자세한 내용은 [파일 전송: 로컬 Windows 또는 MAC PC를 Linux Amazon EC2로](#) 참조하세요.

필수 데이터:

- 접속 DNS 표시 이름 또는 IP 주소:에 설명된 대로 DNS 표시 이름을 사용하거나에 설명된 대로 접속 IP 주소를 [DNS 친화적인 접속 이름](#) 찾습니다 [접속 IP 주소 사용](#).

Note

Amazon EC2 Auto Scaling 그룹을 통해 생성된 Amazon EC2 인스턴스에는 IP 주소가 순환 및 순환 해제되므로 Amazon EC2 콘솔을 사용하여 해당 IP 주소를 찾아야 합니다.

- 사용자 이름(예: `DOMAIN_FQDN\USERNAME`) 및 암호: 계정의 자격 증명. `USERNAME`은 Active Directory 사용자 이름이어야 합니다.

username@customerdomain.com 형식의 사용자 이름을 사용할 수 있지만 PBIS 설정에 문제가 발생할 수 있습니다.

- 스택 IP 주소: 스택을 시작하기 위해 제출한 RFC의 실행 출력을 보거나 Amazon EC2 콘솔에서 Amazon EC2 인스턴스 IP 주소를 조회하여 이를 찾습니다. 단일 Amazon EC2 인스턴스의 경우 AMS SKMS 명령 ListStackSummaries를 사용하여 스택 ID를 찾은 다음 GetStack을 사용하여 스택 IP 주소를 찾을 수도 있습니다. AMS SKMS API 참조는 AWS 아티팩트 콘솔의 보고서 탭을 참조하세요.

필요에 따라 SSH 또는 RDP의 접속 IP 주소에 액세스하고 다음 절차 중 하나를 사용하여 로그인합니다.

Note

RDP 접속은 두 개의 동시 연결만 허용합니다. 따라서 가장 좋은 시나리오에서는 4명의 관리자만 동시에 Windows 스택에 연결할 수 있습니다. RDP에 대한 추가 연결이 필요한 경우 [AMS 온보딩 가이드의 애플리케이션 마이그레이션/온보딩 중 AMS 접속 옵션](#)을 참조하세요.

Linux 컴퓨터에서 Linux 인스턴스로

SSH를 사용하여 SSH 접속에 연결한 다음 Linux 인스턴스에 연결합니다.

MALZ

친숙한 접속 이름에 대한 자세한 내용은 [DNS 접속을 참조하세요](#).

Linux 인스턴스에 연결하려면 먼저 SSH 접속에 연결해야 합니다.

1. 셸 창을 열고 다음을 입력합니다.

```
ssh Domain_FQDN\Username@SSH_bastion_name  
or SSH_bastion_IP
```

Domain_FQDN이 "corp.domain.com"이고, 계정 번호가 "123456789123"이고, Your_Domain이 "amazonaws.com"이고, Bastion "4"를 선택하고, 사용자 이름이 "JoeSmith"인 경우 다음과 같습니다.


```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. 회사 Active Directory 자격 증명으로 로그인합니다.
3. Bash 프롬프트가 표시되면 인스턴스에 SSH를 입력한 다음 다음을 입력합니다.

```
ssh Domain_FQDN\\Username@Instance_IP
```

또는 로그인 플래그(-l)를 사용할 수 있습니다.

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

친숙한 접속 이름에 대한 자세한 내용은 [DNS 접속을 참조하세요](#).

Linux 인스턴스에 연결하려면 먼저 SSH 접속에 연결해야 합니다.

1. 셸 창을 열고 다음을 입력합니다.

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name  
or SSH_BASTION_IP
```

계정 번호가 123456789123이고 Bastion 4를 선택하며 사용자 이름이 JoeSmith인 경우 다음과 같습니다.

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. 회사 Active Directory 자격 증명으로 로그인합니다.
3. Bash 프롬프트가 표시되면 인스턴스에 SSH를 입력한 다음 다음을 입력합니다.

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

또는 로그인 플래그(-l)를 사용할 수 있습니다.

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Linux 컴퓨터에서 Windows 인스턴스로

SSH 터널과 RDP 클라이언트를 사용하여 Linux 컴퓨터에서 Windows 인스턴스에 연결합니다.

MALZ

이 절차에서는 Linux용 원격 데스크톱 연결 클라이언트가 필요합니다. 이 예제에서는 Microsoft 원격 데스크톱(Windows 원격 데스크톱 서비스에 연결하기 위한 오픈 소스 UNIX 클라이언트)을 사용합니다. Rdesktop이 대안입니다.

Note

Windows 인스턴스에 로그인하는 방법은 사용 중인 원격 데스크톱 클라이언트에 따라 변경될 수 있습니다.

먼저 SSH 터널을 설정한 다음 로그인합니다.

친숙한 접속 이름에 대한 자세한 내용은 섹션을 참조하세요 [DNS 친화적인 접속 이름](#).

시작하기 전:

- 연결하려는 인스턴스에 대한 액세스를 요청합니다. 자세한 내용은 [액세스 요청](#)을 참조하세요.
- 연결할 친숙한 DNS SSH 접속 이름을 선택합니다. 예:

```
sshbastion(1-4).Your_Domain
```

Domain_FQDN이 "corp.domain.com"이고, AMS 관리형 Your_Domain이 "amazonaws.com"이고, Bastion "4"를 선택하고, 사용자 이름이 "JoeSmith"인 경우 다음과 같습니다.

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- 연결하려는 인스턴스의 IP 주소를 찾습니다. 자세한 내용은 [인스턴스 ID 또는 IP 주소 찾기를 참조하세요](#).

1. Linux 데스크톱에서 Windows 인스턴스로 연결되는 SSH 터널을 통해 RDP를 설정합니다. 올바른 값으로 ssh 명령을 실행하려면 다음과 같은 몇 가지 방법으로 진행할 수 있습니다.

- Linux 셸에서 변수를 설정한 다음 SSH 연결 명령을 입력합니다.

```
BASTION="sshbastion(1-4).Your_Domain""
WINDOWS="Windows_Instance_Private_IP"
AD="AD_Account_Number"
USER="AD_Username"
ssh -L 3389:$WINDOWS:3389 A$AD\\$USER@$BASTION
```

다음 값이 사용되는 경우의 예:

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- 변수 값을 ssh 명령에 직접 추가합니다.

어느 경우든 렌더링된 요청은 다음과 같습니다(동일한 변수 값 집합을 가정).

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\john.doe@myamsadomain.com
```

2. 다음 중 하나: 원격 데스크톱 클라이언트를 열고 루프백 주소 및 포트 127.0.0.1:3389를 입력한 다음 연결을 엽니다.

또는 새 Linux 데스크톱 셸에서 Windows 인스턴스에 로그인합니다. RDesktop을 사용하는 경우 명령은 다음과 같습니다.

```
rdesktop 127.0.0.1:3389
```

Windows 인스턴스의 원격 데스크톱 창이 Linux 데스크톱에 나타납니다.

Tip

원격 데스크톱 세션이 시작되지 않는 경우 SSH 접속에서 Windows 인스턴스로의 네트워크 연결이 1단계의 셸에서 포트 3389에서 허용되는지 확인합니다 (private_ip_address_of_windows_instance 적절하게 교체).

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

성공:

```
nc 172.16.0.83 3389 -v -z
    Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp    0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

SALZ

단일 계정 랜딩 존에 대한이 절차를 수행하려면 Linux용 원격 데스크톱 연결 클라이언트가 필요합니다. 이 예제에서는 Microsoft 원격 데스크톱(Windows 원격 데스크톱 서비스에 연결하기 위한 오픈 소스 UNIX 클라이언트)을 사용합니다. Rdesktop이 대안입니다.

Note

Windows 인스턴스에 로그인하는 방법은 사용 중인 원격 데스크톱 클라이언트에 따라 변경될 수 있습니다.

먼저 SSH 터널을 설정한 다음 로그인합니다.

친숙한 접속 이름에 대한 자세한 내용은 섹션을 참조하세요 [DNS 친화적인 접속 이름](#).

시작하기 전:

- 연결하려는 인스턴스에 대한 액세스를 요청합니다. 자세한 내용은 [액세스 요청](#)을 참조하세요.
- 연결할 친숙한 DNS SSH 접속 이름을 선택합니다. 예:

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

계정 번호가 123456789123이고 Bastion 4를 선택한 경우 다음과 같습니다.

```
sshbastion4.A123456789123.amazonaws.com
```

- 연결하려는 인스턴스의 IP 주소를 찾습니다. 자세한 내용은 [인스턴스 ID 또는 IP 주소 찾기를 참조하세요](#).

1. Linux 데스크톱에서 Windows 인스턴스로 연결되는 SSH 터널을 통해 RDP를 설정합니다. 올바른 값으로 ssh 명령을 실행하려면 다음과 같은 몇 가지 방법으로 진행할 수 있습니다.
- Linux 셸에서 변수를 설정한 다음 SSH 연결 명령을 입력합니다.

```
BASTION="sshbastion(1-4).AMSAccountNumber.amazonaws.com"
WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
AD="AD_ACCOUNT_NUMBER"
USER="AD_USERNAME"
ssh -L 3389:$WINDOWS:3389 A$AD\\$USER@$BASTION
```

다음 값이 사용되는 경우의 예:

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- 변수 값을 ssh 명령에 직접 추가합니다.

어느 경우든 렌더링된 요청은 다음과 같습니다(동일한 변수 값 집합을 가정).

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. 다음 중 하나: 원격 데스크톱 클라이언트를 열고 루프백 주소 및 포트 127.0.0.1:3389를 입력한 다음 연결을 엽니다.

또는 새 Linux 데스크톱 셸에서 Windows 인스턴스에 로그인합니다. RDesktop을 사용하는 경우 명령은 다음과 같습니다.

```
rdesktop 127.0.0.1:3389
```

Windows 인스턴스의 원격 데스크톱 창이 Linux 데스크톱에 나타납니다.

i Tip

원격 데스크톱 세션이 시작되지 않는 경우 SSH 접속에서 Windows 인스턴스로의 네트워크 연결이 1단계의 셸에서 포트 3389에서 허용되는지 확인합니다 (private_ip_address_of_windows_instance 적절하게 교체).

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

성공:

```
nc 172.16.0.83 3389 -v -z
Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp    0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

Windows 컴퓨터에서 Windows 인스턴스로

Windows 원격 데스크톱 연결 클라이언트를 사용하여 Windows 컴퓨터에서 Windows 인스턴스에 연결합니다.

MALZ

친숙한 접속 이름에 대한 자세한 내용은 섹션을 참조하세요 [DNS 친화적인 접속 이름](#).

1. 표준 Windows 프로그램인 원격 데스크톱 연결 프로그램을 열고 호스트 이름 필드에 Windows 접속의 친숙한 DNS 이름을 입력합니다.
2. 연결을 선택합니다. 원격 데스크톱 연결은 접속에 대한 RDP 연결을 시도합니다.

성공하면 자격 증명 대화 상자가 열립니다. 액세스 권한을 얻으려면 Windows 인스턴스와 마찬가지로 회사 Active Directory 자격 증명을 사용합니다.

3. 접속에서 원격 데스크톱 연결 프로그램을 열고 연결하려는 Windows 인스턴스의 IP 주소(예: 10.0.0.100)를 입력한 다음 연결을 선택합니다. Windows 인스턴스에 연결하기 전에 회사 Active Directory 자격 증명이 다시 필요합니다.

SALZ

친숙한 접속 이름에 대한 자세한 내용은 섹션을 참조하세요 [DNS 친화적인 접속 이름](#).

1. 표준 Windows 프로그램인 원격 데스크톱 연결 프로그램을 열고 호스트 이름 필드에 Windows Bastion의 친숙한 DNS 이름을 입력합니다. 예를 들어, 계정 번호가 123456789123이고 Bastion 4를 선택하면 다음과 같습니다 `rdpbastion(1-4).AMSAccountNumber.amazonaws.com` 같습니다 `rdpbastion4.A123456789123.amazonaws.com`.

2. 연결을 선택합니다. 원격 데스크톱 연결은 접속에 대한 RDP 연결을 시도합니다.

성공하면 자격 증명 대화 상자가 열립니다. 액세스 권한을 얻으려면 Windows 인스턴스와 마찬가지로 회사 Active Directory 자격 증명을 사용합니다.

3. 접속에서 원격 데스크톱 연결 프로그램을 열고 연결하려는 Windows 인스턴스의 IP 주소(예: 10.0.0.100)를 입력한 다음 연결을 선택합니다. Windows 인스턴스에 연결하기 전에 회사 Active Directory 자격 증명이 다시 필요합니다.

Windows 컴퓨터에서 Linux 인스턴스로

Windows 환경에서 SSH 접속으로 RDP하려면 다음 단계를 따릅니다.

MALZ

시작하기 전:

- 연결하려는 인스턴스에 대한 액세스를 요청합니다. 자세한 내용은 [액세스 요청](#)을 참조하세요.
- 연결할 친숙한 DNS SSH 접속 이름을 선택합니다. 예:

```
sshbastion(1-4).YOUR_DOMAIN
```

YOUR_DOMAIN이 myamsaddomain.com"이고 Bastion 4를 선택하면 다음과 같습니다.

```
sshbastion4.myamsaddomain.com
```

- 연결하려는 인스턴스의 IP 주소를 찾습니다. 자세한 내용은 [인스턴스 ID 또는 IP 주소 찾기를 참조하세요](#).

Windows 시스템에서 Linux 인스턴스에 연결하려면 먼저 SSH 접속에 연결해야 합니다.

기본 Windows [OpenSSH 클라이언트](#)를 사용하거나 로컬 시스템에 [PuTTY](#)를 설치합니다. OpenSSH에 대한 자세한 내용은 [Windows의 OpenSSH](#)를 참조하세요.

1. 기본 Windows를 사용하거나 PuTTY를 열고 SSH 접속 호스트 이름 또는 SSH 접속의 IP 주소를 입력합니다. 예를 들어 10.65.2.214(22는 SSH에 사용되는 포트이며 기본적으로 설정됨)입니다.
2. OpenSSH 또는 PuTTY는 접속에 대한 SSH 연결을 시도하고 셸 창을 엽니다.
3. RDP 호스트와 마찬가지로 회사 Active Directory 자격 증명을 사용하여 액세스 권한을 얻습니다.
4. Bash 프롬프트가 표시되면 인스턴스로 SSH합니다. 입력:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

시작하기 전:

- 연결하려는 인스턴스에 대한 액세스를 요청합니다. 자세한 내용은 [액세스 요청](#)을 참조하세요.
- 연결할 친숙한 DNS SSH 접속 이름을 선택합니다. 예:

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

계정 번호가 123456789123이고 Bastion 4를 선택한 경우 다음과 같습니다.

```
sshbastion4.A123456789123.amazonaws.com
```

- 연결하려는 인스턴스의 IP 주소를 찾습니다. 자세한 내용은 [인스턴스 ID 또는 IP 주소 찾기를 참조하세요](#).

Windows 시스템에서 Linux 인스턴스에 연결하려면 먼저 SSH 접속에 연결해야 합니다.

기본 Windows [OpenSSH 클라이언트](#)를 사용하거나 로컬 시스템에 [PuTTY](#)를 설치합니다. OpenSSH에 대한 자세한 내용은 [Windows의 OpenSSH](#)를 참조하세요.

1. 기본 Windows를 사용하거나 PuTTY를 열고 SSH 접속 호스트 이름 또는 SSH 접속의 IP 주소를 입력합니다. 예를 들어 10.65.2.214(22는 SSH에 사용되는 포트이며 기본적으로 설정됨)입니다.
2. OpenSSH 또는 PuTTY는 접속에 대한 SSH 연결을 시도하고 셸 창을 엽니다.
3. RDP 호스트와 마찬가지로 회사 Active Directory 자격 증명을 사용하여 액세스 권한을 얻습니다.
4. Bash 프롬프트가 표시되면 인스턴스로 SSH합니다. 입력:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

AMS 계정의 팀 또는 역할 기반 액세스 제어

시나리오: 두 애플리케이션 팀 A와 B는 각각 앱 "AA" 및 "BB"에 단일 AMS 계정을 사용합니다. 팀 A는 앱 "AA"의 리소스에만 액세스하고, 팀 B는 앱 "BB"의 리소스에만 액세스하려고 합니다. 어떻게 설정하나요?

ITSM의 도구를 사용하여 팀 기반 액세스 제어(TBAC)를 구현합니다. 예를 들어 AMS API와의 통합을 위해 AMS ServiceNow APIs. 이 구현에 대한 상위 수준 지침은 CSDM에 문의하십시오.

AMS Advanced의 자동 인스턴스 구성

AMS Advanced 자동 인스턴스 구성 서비스는 매일 실행되며 관리형 EC2 인스턴스에서 SSM 및 CloudWatch 에이전트와 구성 파일을 자동으로 스캔하고 업데이트합니다. 필요에 따라 업데이트가 적용됩니다.

- SSM 및 CloudWatch 에이전트
- CloudWatch 구성 파일

이러한 업데이트를 통해 AMS는 AMS 관리형 EC2 인스턴스에 액세스하고 적절한 [로그](#) 및 지표를 내보내도록 인스턴스를 구성할 수 있습니다.

주제

- [자동 인스턴스 구성을 위한 사전 조건](#)
- [SSM 에이전트 자동 설치](#)
- [자동 변경 사항](#)

자동 인스턴스 구성을 위한 사전 조건

변경 관리를 사용하여 인스턴스를 배포하는 AMS Advanced 고객의 경우 다음 사전 조건을 충족해야 합니다.

- SSM 에이전트는 관리형 상태로 설치됩니다.
- 인스턴스에는 관리형 인스턴스로 태그가 지정됩니다. (aws:cloudformation:stack-name태그의 값은 stack- 또는 로 시작합니다sc-.)

SSM 에이전트가 아직 인스턴스에 설치되지 않은 경우 AMS SSM 에이전트 자동 설치 기능을 사용하여 설치할 수 있습니다. 자세한 내용은 [SSM 에이전트 자동 설치](#) 단원을 참조하십시오.

또는 SSM 에이전트를 수동으로 설치할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- Linux: [Linux용 EC2 인스턴스에 SSM 에이전트 수동 설치 - AWS Systems Manager](#)
- Windows: [Windows Server용 EC2 인스턴스에 SSM 에이전트 수동 설치 - AWS Systems Manager](#)

SSM 에이전트에 대한 자세한 내용은 AWS 설명서 [SSM 에이전트 작업을](#) 참조하세요.

SSM 에이전트 자동 설치

AMS가 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 관리하도록 하려면 각 인스턴스에 AWS Systems Manager SSM 에이전트를 설치해야 합니다. 인스턴스에 SSM 에이전트가 설치되어 있지 않은 경우 AMS SSM 에이전트 자동 설치 기능을 사용할 수 있습니다.

Note

- 이 기능은 Auto Scaling 그룹에 없고 AMS에서 지원하는 Linux 운영 체제를 실행하는 EC2 인스턴스에서만 사용할 수 있습니다.
- AMS SSM 에이전트 자동 설치 기능은 기본적으로 비활성화되어 있습니다. 활성화하려면 CA 또는 CSDM에 문의하세요.

SSM 에이전트 사용을 위한 사전 조건

- 대상 인스턴스와 연결된 인스턴스 프로파일에 다음 정책(또는 허용 목록에 있는 것과 동등한 권한) 중 하나가 있는지 확인합니다.
 - AmazonSSMManagedEC2InstanceDefaultPolicy
 - AmazonSSMManagedInstanceCore
- 이전 정책에 나열된 권한을 명시적으로 거부하는 AWS Organizations 수준의 서비스 제어 정책이 없는지 확인합니다.

자세한 내용은 [Systems Manager에 필요한 인스턴스 권한 구성](#)을 참조하세요.

- 아웃바운드 트래픽을 차단하려면 대상 인스턴스가 있는 VPC에서 다음 인터페이스 엔드포인트가 활성화되어 있는지 확인합니다(URL의 "리전"을 적절하게 바꿉니다).
 - ssm.<region>.amazonaws.com
 - ssmmessages.<region>.amazonaws.com
 - ec2messages.<리전>.amazonaws.com

자세한 내용은 [Systems Manager용 VPC 엔드포인트를 사용하여 EC2 인스턴스의 보안 개선](#)을 참조하세요.

관리형 노드 가용성 활성화 또는 문제 해결에 대한 일반적인 팁은 [솔루션 2: 인스턴스에 대해 IAM 인스턴스 프로파일이 지정되었는지 확인\(EC2 인스턴스만 해당\)](#)을 참조하세요.

Note

AMS는 자동 설치 프로세스의 일부로 각 인스턴스를 중지하고 시작합니다. 인스턴스가 중지되면 인스턴스 스토어 볼륨에 저장된 데이터와 RAM에 저장된 데이터가 손실됩니다. 자세한 내용은 [인스턴스를 중지하면 어떻게 되는지를 참조하세요](#).

인스턴스에 SSM 에이전트 자동 설치 요청

계정이 AMS Accelerate 패치 추가 기능에 온보딩된 경우 인스턴스에 대한 패치 유지 관리 기간(MW)을 구성합니다. 패치 프로세스를 완료하려면 작동 중인 SSM 에이전트가 필요합니다. 인스턴스에 SSM 에이전트가 없는 경우 AMS는 패치 유지 관리 기간 동안 인스턴스를 자동으로 설치하려고 시도합니다.

Note

AMS는 자동 설치 프로세스의 일부로 각 인스턴스를 중지하고 시작합니다. 인스턴스가 중지되면 인스턴스 스토어 볼륨에 저장된 데이터와 RAM에 저장된 데이터가 손실됩니다. 자세한 내용은 [인스턴스를 중지하면 어떻게 되는지를 참조하세요](#).

SSM 에이전트 자동 설치 작동 방식

AMS는 EC2 사용자 데이터를 사용하여 인스턴스에서 설치 스크립트를 실행합니다. 사용자 데이터 스크립트를 추가하고 인스턴스에서 실행하려면 AMS가 각 인스턴스를 중지하고 시작해야 합니다.

인스턴스에 기존 사용자 데이터 스크립트가 이미 있는 경우 AMS는 자동 설치 프로세스 중에 다음 단계를 완료합니다.

1. 기존 사용자 데이터 스크립트의 백업을 생성합니다.
2. 기존 사용자 데이터 스크립트를 SSM 에이전트 설치 스크립트로 바꿉니다.
3. 인스턴스를 다시 시작하여 SSM 에이전트를 설치합니다.
4. 인스턴스를 중지하고 원래 스크립트를 복원합니다.
5. 원래 스크립트로 인스턴스를 다시 시작합니다.

자동 변경 사항

AMS Advanced 자동 인스턴스 구성 서비스는 필요에 따라 EC2 인스턴스를 변경합니다.

변경 사항:

- [Linux 인스턴스에서 코드 자동 업데이트](#)
- [Linux 인스턴스에서 PBIS 자동 업데이트](#)
- [SSM 및 CloudWatch 에이전트의 최소 버전 자동 업데이트](#)
- [CloudWatch 구성 파일, 세부 정보 업데이트](#)
- [자동으로 구성된 로그](#)

Linux 인스턴스에서 코드 자동 업데이트

AMS는 Linux 인스턴스의 인스턴스 코드에 대해 자동으로 업데이트됩니다. 이를 통해 AMS 구성 요소 및 환경의 운영 안정성과 보안을 모두 개선할 수 있습니다.

FAQ:

Linux의 온 인스턴스 코드(OIC)에는 무엇이 포함되나요?

OIC에는 일부 구성 파일 및 cron 작업과 함께 `ams-toolkit` 패키지가 포함되어 있습니다. AMS에는 통합을 위해 이러한 파일 및 패키지가 필요합니다(Active Directory, CloudFormation 및 기타 종속성). 워크로드 수집 중에 이러한 파일을 AMS 제공 AMIs로 미리 베이킹하거나 인스턴스에 설치합니다.

AMS는 언제 OIC를 업데이트합니까?

AMS는 버그 수정 또는 기타 개선 사항이 포함된 새 버전을 릴리스할 때 OIC를 업데이트합니다. OIC 버전 및 업데이트를 확인하는 워크플로는 매일 실행됩니다.

Linux 인스턴스에서 PBIS 자동 업데이트

AMS는 Power Broker Identity Service(PBIS) 모듈을 사용하여 Linux 인스턴스를 AMS 관리형 Active Directory에 조인합니다.

AMS는 Linux 인스턴스의 PBIS를 자동으로 업데이트합니다.

FAQ:

AMS는 언제 PBIS를 업데이트하나요?

AMS는 재부팅 시 PBIS 업데이트를 켭니다. 사용 가능한 새 PBIS 버전이 있는 경우 AMS는 다음 인스턴스 재부팅 중에 새 버전을 설치하려고 시도합니다.

PBIS 업데이트를 끌 수 있나요?

인스턴스 또는 계정 수준에서 PBIS 업데이트를 끌 수 있습니다.

- 계정 수준: SSM 파라미터 스토어에서 파라미터를 생성합니다. 이름: `/ams/skip-pbis-update`, 값: `true` (모든 경우).

Note

인스턴스 프로파일에는 SSM 파라미터를 읽을 수 있는 권한이 있어야 합니다. 플래그가 누락된 경우 기본 동작은 업데이트를 실행하는 것입니다.

- 인스턴스 수준:
 - 태그 기반: 인스턴스에 Key: `skip_pbis_update`, Value: `true` (모든 사례) 태그를 추가합니다.
 - Config 파일: `/opt/aws/ams/etc/ams.conf.d/state.ini` 파일에 다음 플래그를 추가합니다. `skip_pbis_update = true`.

Note

태그는 SSM 파라미터보다 우선 순위가 높습니다. 파라미터를 통해 계정 수준에서 PBIS 업데이트를 비활성화할 수 있지만 태그, Key: `skip_pbis_update`를 추가하여 단일(또는 여러) 인스턴스에 대해 PBIS 업데이트를 비활성화할 수 있습니다. Value: `false`.

설명된 옵션 중 하나를 구성하려면 AMS 환경의 표준 변경 관리 프로세스를 따릅니다.

SSM 및 CloudWatch 에이전트의 최소 버전 자동 업데이트

AMS Advanced 최소 버전(SSM 또는 CloudWatch 에이전트)은 AMS 서비스 팀에서 테스트하고 운영 체제에 대해 사전 승인된 버전입니다. 사전 예방을 유지하고 안정적이고 호환되는 최신 버전을 실행하기 위해 노력하므로 버전 번호는 시간이 지남에 따라 변경됩니다. AMS에 서비스 요청을 제출하여 현재 최소 버전을 찾을 수 있습니다.

• SSM 에이전트 관리

Amazon SSM 에이전트는 인스턴스에서 원격 명령을 실행할 책임이 있습니다. 인스턴스 구성 자동화는 SSM 에이전트가 최소 버전을 실행하고 있는지 확인합니다.

- Cloudwatch 에이전트 관리

Amazon CloudWatch 에이전트는 OS 로그 및 지표를 내보낼 책임이 있습니다. 자동 인스턴스 구성은 다음을 수행합니다.

- 필요한 경우는 레거시 CloudWatch Log 에이전트를 비활성화하고 구성을 새 통합 CloudWatch 에이전트로 마이그레이션합니다.
- 인스턴스가 레거시 CloudWatch Log Agent를 실행하는 경우 자동 인스턴스 구성은 레거시 CloudWatch Log 에이전트 서비스를 비활성화하고 해당 구성을 통합 CloudWatch 에이전트로 마이그레이션합니다.
- CloudWatch 구성을 사용자 지정하여 적절한 로그와 지표를 내보냅니다.

영향을 받는 파일 및 디렉터리:

- Windows
 - %ProgramData%\Amazon\AmazonCloudWatchAgent\
 - %ProgramData%\Amazon\AmazonCloudWatchAgent\Configs\
- Linux
 - /opt/aws/amazon-cloudwatch-agent/등
 - /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

CloudWatch 구성 파일, 세부 정보 업데이트

다음 CloudWatch 디렉터리([권장 디렉터리 참조](#))에서 사용자 지정 CloudWatch 구성(JSON만 해당)을 읽고 표준 AMS CloudWatch 구성과 병합합니다.

- CloudWatch 파일
 - 인스턴스에서:
 - Windows
 - %ProgramData%\Amazon\AmazonCloudWatchAgent\Configs\
 - %ProgramFiles%\WindowsPowerShell\Modules\AWSManagedServices.Logging.Utilities\Files\Config.json
 - Linux
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

- Windows:
 - https://ams-configuration-artifacts-REGION_NAME.s3.REGION_NAME.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json
- Linux:
 - https://ams-configuration-artifacts-REGION_NAME.s3.REGION_NAME.amazonaws.com/configurations/cloudwatch/latest/linux-cloudwatch-config.json

자동으로 구성된 로그

다음 로그를 작성하도록 인스턴스를 구성합니다.

- Windows:
 - AmazonSSMAgentLog
 - AmazonCloudWatchAgentLog
 - AmazonSSMErrorLog
 - AmazonCloudFormationLog
 - ApplicationEventLog
 - EC2ConfigServiceEventLog
 - MicrosoftWindowsAppLockerEXEAndDLLEventLog
 - MicrosoftWindowsAppLockerMSIAndScriptEventLog
 - MicrosoftWindowsGroupPolicyOperationalEventLog
 - SecurityEventLog
 - SystemEventLog
- Linux:
 - /var/log/amazon/ssm/amazon-ssm-agent.log
 - /var/log/amazon/ssm/errors.log
 - /var/log/audit/audit.log
 - /var/log/cloud-init-output.log
 - /var/log/cloud-init.log
 - /var/log/cron
 - /var/log/dpkg.log
 - /var/log/maillog

- /var/log/messages
- /var/log/secure
- /var/log/spooler
- /var/log/syslog
- /var/log/yum.log
- /var/log/zypper.log

AMS의 모니터링 및 이벤트 관리

주제

- [모니터링이란 무엇입니까?](#)
- [AMS 모니터링 시스템은 무엇을 모니터링합니까?](#)
- [모니터링 작동 방식](#)
- [AMS 계정에 대한 모니터링 구성 보기](#)
- [AMS 계정에 대한 모니터링 구성 변경](#)
- [AMS의 애플리케이션 인식 인시던트 알림](#)
- [AMS에서 OpsCenter 사용](#)
- [AMS의 알림](#)
- [AMS에서 추가 CloudWatch 경보 생성](#)
- [AMS에서 사용자 지정 CloudWatch 지표 및 경보 생성](#)
- [AMS에서 .Net 및 SQL Server용 CloudWatch Application Insights 사용](#)
- [AMS에서 Amazon EventBridge 관리형 규칙 사용](#)
- [AMS의 신뢰할 수 있는 수정자](#)

AWS Managed Services(AMS) 모니터링 시스템은 AMS 리소스의 장애, 성능 저하 및 보안 문제를 모니터링합니다. AMS 모니터링 시스템은 Amazon CloudWatch(CloudWatch), Amazon GuardDuty, Amazon Macie, 등의 AWS 서비스를 사용합니다. AWS Health. 모니터링 시스템 외에도 AMS는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 맬웨어로부터 보호하기 위해 TrendMicro DeepSecurity를 배포합니다. 엔드포인트 보안(EPS) 기본값에 대한 자세한 내용은 섹션을 참조하세요 [엔드포인트 보안\(EPS\)](#).

AMS 모니터링은 다음과 같은 이점을 제공합니다.

- 관리형 계정에 대한 다른 모니터링을 구성하지 않더라도 기본 보호 수준을 갖도록 하는 모니터링 기준입니다. 자세한 내용은 [AMS의 기준 모니터링 알림](#) 단원을 참조하세요.
- 적절한 조치를 결정하기 위한 조사 알림입니다. 예를 들어 GuardDuty가 Amazon EC2 인스턴스에 대한 무차별 강제 시도를 나타내는 활동을 발견하면 AMS는 VPC 플로우로그를 분석하여 활동의 오리진과 컨텍스트를 이해합니다.
- 애플리케이션에 미치는 영향을 방지하거나 줄이기 위해 가능한 경우 알림을 수정합니다. 예를 들어 독립 실행형 Amazon EC2 인스턴스를 사용 중이고 시스템 상태 확인에 실패한 경우 AMS는 인스턴

스를 중지했다가 다시 시작하여 인스턴스 복구를 시도합니다. 자세한 내용은 [알림의 AMS 자동 문제 해결](#) 단원을 참조하십시오.

- OpsCenter를 사용하여 활성 및 이전에 해결된 알림으로의 투명성. 예를 들어 Amazon EC2 인스턴스에서 CPU 사용률이 예기치 않게 높은 경우 AWS Systems Manager 콘솔에 대한 액세스 (OpsCenter 콘솔에 대한 액세스 포함)를 요청하고 OpsCenter 콘솔에서 직접 OpsItem을 볼 수 있습니다. OpsCenter

모니터링이란 무엇입니까?

AMS 모니터링 시스템은 AWS 리소스에 장애, 성능 저하 및 보안 문제가 있는지 모니터링합니다. 관리형 계정인 AMS는 해당 AWS 리소스에 대한 경보를 구성 및 배포하고 모니터링하며 해당하는 경우 문제 해결을 수행합니다.

AMS 모니터링 시스템은 계정의 모니터링 구성을 기반으로 알림을 생성합니다. 계정의 모니터링 구성은 알림을 생성하는 계정의 모든 리소스 파라미터를 나타냅니다. 리소스 파라미터에 대한 자세한 내용은 섹션을 참조하세요 [AMS의 기본 모니터링 알림](#). 계정의 모니터링 구성에는 CloudWatch 경보 정의와 알림을 생성하는 CloudWatch 이벤트 규칙(경보 또는 이벤트)이 포함됩니다.

기본 모니터링 구성은 관리형 계정의 리소스를 모니터링하기 위해 AMS에서 큐레이션한 경보 정의 ([AMS의 기본 모니터링 알림](#)) 세트입니다. 계정의 모니터링 구성은 사용자가 요청한 변경 사항으로 인해 기본 구성과 다를 수 있습니다.

계정에 구성된 기본 모니터링에 의해 생성된 임박한 장애, 진행 중인 장애, 후퇴 또는 잠재적 장애, 성능 저하 또는 보안 문제에 대한 알림을 알림이라고 합니다. 알림의 예로는 Amazon CloudWatch 경보, Amazon CloudWatch 이벤트, 이벤트 또는 Amazon GuardDuty와 같은 AWS 서비스의 결과, Trend Micro Deep Security의 이벤트 또는 알림이 있습니다.

Amazon GuardDuty, Amazon Macie 또는 Trend Micro Deep Security와 같은 보안 관련 AWS 서비스의 알림을 보안 알림이라고 하여 다른 유형의 알림과 구분합니다.

AMS 모니터링은 다음과 같은 이점을 제공합니다.

- 요구 사항에 맞게 기본 리소스 경보를 사용자 지정하는 기능입니다.
- 애플리케이션에 미치는 영향을 방지하거나 줄이기 위해 가능한 경우 알림을 자동으로 수정합니다. 예를 들어 독립 실행형 Amazon EC2 인스턴스를 사용 중이고 시스템 상태 확인에 실패한 경우 AMS는 인스턴스를 중지했다가 다시 시작하여 인스턴스 복구를 시도합니다. 자세한 정보는 [알림의 AMS 자동 문제 해결](#)을 참조하십시오.

- OpsCenter를 사용하여 활성 및 이전에 해결된 알림으로의 투명성. 예를 들어 Amazon EC2 인스턴스에서 CPU 사용률이 예기치 않게 높은 경우 콘솔에 AWS Systems Manager 대한 액세스 (OpsCenter 콘솔에 대한 액세스 포함)를 요청하고 OpsCenter 콘솔에서 직접 OpsItem을 볼 수 있습니다. OpsCenter
- 알림을 조사하여 적절한 조치를 결정합니다.
- 계정 및 지원되는 AWS 서비스의 구성을 기반으로 생성된 알림입니다. 계정의 모니터링 구성은 알림을 생성하는 계정의 모든 리소스 파라미터를 나타냅니다. 계정의 모니터링 구성에는 CloudWatch 경보 정의와 알림(경보 또는 이벤트)을 생성하는 EventBridge(이전에는 CloudWatch Events라고 함)가 포함됩니다. 리소스 파라미터에 대한 자세한 내용은 섹션을 참조하세요 [AMS의 기준 모니터링 알림](#).
- 임박, 진행 중, 후퇴 또는 잠재적 장애, 성능 저하 또는 계정에 구성된 기준 모니터링에서 생성된 보안 문제에 대한 알림(알림이라고 함). 알림의 예로는 CloudWatch 경보, 이벤트 또는 GuardDuty 또는 같은 AWS 서비스의 결과가 있습니다 AWS Health.

AMS 모니터링 시스템은 무엇을 모니터링합니까?

AWS Managed Services(AMS) 공유 서비스 책임 모델에 따라 AMS 모니터링 시스템은 AWS 인프라를 모니터링합니다. 모니터링되는 AWS 리소스 및 각 리소스에 대한 알림 유형을 포함하여 AMS의 기준 모니터링에 대한 자세한 내용은 섹션을 참조하세요 [AMS의 기준 모니터링 알림](#). Amazon EC2 인스턴스의 경우 AMS는 운영 체제를 모니터링하고 CPU 사용률 및 루트 볼륨 사용량과 같은 OS 지표를 기반으로 기준 모니터링을 제공합니다.

애플리케이션에 맞는 AWS 서비스를 사용하여 추가 모니터링으로 AMS 모니터링을 보완하는 것이 좋습니다. 가용성 모니터링에 대한 지침은 이 백서 [신뢰성 원칙](#)의 "모니터링 및 경보" 섹션을 참조하세요. 운영 요구 사항에 맞게 자체 모니터링을 구성할 수 있습니다. 이를 수행하는 방법은 [AMS에서 추가 CloudWatch 경보 생성](#) 및에서 설명합니다 [AMS에서 사용자 지정 CloudWatch 지표 및 경보 생성](#).

AMS에서 Active Directory 신뢰의 단일 계정 랜딩 존 사전 모니터링

AMS 단일 계정 랜딩 존(SALZ)은 AMS 관리형 계정의 관리형 Active Directory(AD)와 회사 도메인 간의 단방향 신뢰(들) 상태를 모니터링합니다. Managed AD와의 단방향 신뢰는 액세스 요청 및 인스턴스 로그인 요청에 매우 중요합니다. 이 새로운 모니터링을 통해 AMS는 이제 신뢰 관련 문제에 사전에 대응하고 액세스 관련 인시던트를 감지하는 데 걸리는 평균 시간을 줄입니다.

이 기능은 AWS Managed Services(AMS) 계정에서 자동으로 활성화됩니다.

약간의 비용 영향이 있습니다. 이 기능은 4개의 AWS CloudWatch 지표와 1개의 신뢰에 대한 2개의 AWS CloudWatch 경보를 사용합니다.

모니터링 작동 방식

AWS Managed Services(AMS)의 모니터링 아키텍처에 대한 다음 그래픽을 참조하세요.

다음 다이어그램은 AMS 다중 계정 랜딩 존 및 AMS 단일 계정 랜딩 존 모니터링 워크플로에 대한 개략적인 개요를 제공합니다.

- **생성:** 계정 온보딩 시 AMS는 관리형 계정에서 생성된 모든 리소스에 대한 기존 모니터링 (CloudWatch(CW) 경보 및 CW 이벤트 규칙의 조합)을 구성합니다. 기존 모니터링 구성은 CW 경보가 트리거되거나 CW 이벤트가 생성될 때 알림을 생성합니다.
- **집계:**
 - 다중 계정 랜딩 존: 알림은 애플리케이션 및 코어 조직 단위 계정 내의 리소스에서 생성되며 보안 계정을 통해 전달하여 AMS 모니터링 시스템으로 전송됩니다.
 - 단일 계정 랜딩 존: 리소스에서 생성된 모든 알림은 계정의 SNS 주제로 전달하여 AMS 모니터링 시스템으로 전송됩니다.
 - AMS가 EC2 알림을 그룹화하는 방법을 구성할 수도 있습니다. AMS는 동일한 EC2 인스턴스와 관련된 모든 알림을 단일 인시던트로 그룹화하거나 기본 설정에 따라 알림당 하나의 인시던트를 생성합니다. Cloud Service Delivery Manager 또는 Cloud Architect와 협력하여 언제든지 구성을 변경할 수 있습니다. 이는 다중 계정 랜딩 존을 사용하든 단일 계정 랜딩 존을 사용하든 동일한 방식으로 작동합니다.
- **처리 중:** AMS는 알림을 분석하고 영향 가능성을 기반으로 처리합니다. 알림은 다음에 설명된 대로 처리됩니다.
 - 알려진 고객 영향이 있는 알림: 이로 인해 새 인시던트 보고서가 생성되고 AMS는 인시던트 관리 프로세스를 따릅니다. 인시던트 관리에 대한 자세한 내용은 섹션을 참조하세요 [AMS 인시던트 대응](#).

알림 예: Amazon EC2 인스턴스가 시스템 상태 확인에 실패하고 AMS는 인스턴스를 중지했다가 다시 시작하여 인스턴스 복구를 시도합니다.

- 고객에게 미치는 영향이 불확실한 알림: 이러한 유형의 알림의 경우 AMS는 인시던트 보고서를 보내며, 대부분의 경우 AMS가 조치를 취하기 전에 영향을 확인하도록 요청합니다. 그러나 인프라 관련 검사를 통과하면 AMS는 인시던트 보고서를 보내지 않습니다.

예: Amazon EC2 인스턴스에서 10분 이상 >85% CPU 사용률에 대한 알림은 사용량에 따라이 동작이 예상될 수 있으므로 인시던트로 즉시 분류할 수 없습니다. 이 예제에서 AMS Automation은 리소스에 대한 인프라 관련 검사를 수행합니다. 이러한 검사가 통과하면 CPU 사용량이 99%를 초과하더라도 AMS는 알림 알림을 보내지 않습니다. 자동화가 리소스에서 인프라 관련 검사가 실패

하고 있음을 감지하면 AMS는 알림 알림을 보내고 완화가 필요한지 확인합니다. 알림은이 단원에서 자세히 설명합니다. AMS는 알림에서 완화 옵션을 제공합니다. 알림이 인시던트임을 확인하는 알림에 회신하면 AMS가 새 인시던트 보고서를 생성하고 AMS 인시던트 관리 프로세스가 시작됩니다. "고객 영향 없음" 또는 3일 동안 전혀 응답하지 않음 응답을 수신하는 서비스 알림은 해결됨으로 표시되고 해당 알림은 해결됨으로 표시됩니다.

- 고객 영향이 없는 알림: 평가 후 AMS가 알림에 고객에게 영향이 없다고 판단하면 알림이 종료됩니다.

예를 들어,는 교체가 필요하지만 이후 해당 인스턴스가 종료되었음을 EC2 인스턴스에 AWS Health 알립니다.

EC2 인스턴스 그룹화된 알림

동일한 EC2 인스턴스의 알림을 단일 인시던트로 그룹화하도록 AMS 모니터링을 구성할 수 있습니다. Cloud Service Delivery Manager 또는 Cloud Architect가 이를 구성할 수 있습니다. 각 AMS 관리형 계정에 대해 구성할 수 있는 파라미터는 4개입니다.

1. 범위: 계정 전체 또는 태그 기반 중 하나를 선택합니다.

- 해당 계정의 모든 EC2 인스턴스에 적용되는 구성을 지정하려면 범위 = 계정 전체를 선택합니다.
- 특정 태그가 있는 해당 계정의 EC2 인스턴스에만 적용되는 구성을 지정하려면 범위 = 태그 기반을 선택합니다.

2. 그룹화 규칙: 클래식 또는 인스턴스를 선택합니다.

- 계정의 모든 리소스에 대해 인스턴스 수준 그룹화를 구성하려면 범위 = 계정 전체 및 그룹화 규칙 = 인스턴스를 선택합니다.
- 인스턴스 수준 그룹화를 사용하도록 계정의 특정 리소스를 구성하려면 해당 인스턴스에 태그를 지정한 다음 범위 = 태그 기반 및 그룹화 규칙 = 인스턴스 수준을 선택합니다.
- 계정의 알림에 인스턴스 그룹화를 사용하지 않으려면 그룹화 규칙 = 클래식을 선택합니다.

3. 참여 옵션: 없음, 보고서만 또는 기본값을 선택합니다.

- 구성이 활성화 상태인 동안 AMS가 인시던트를 생성하거나 해당 리소스의 경보에 대한 자동화를 실행하지 않도록 하려면 없음을 선택합니다.
- 구성이 활성화되어 있는 동안 AMS가 인시던트를 생성하거나 해당 리소스에서 경보에 대한 자동화를 실행하지 않고 자동 복구 Systems Manager 문서를 실행하지 않고 보고에 이러한 이벤트의 레코드를 포함하려면 보고서만 선택합니다. 이는 상호 작용하는 인시던트 지원 사례의 양을 줄이고 일부 리소스의 일부 인시던트가 비프로덕션 계정의 인시던트와 같이 즉각적인 주의가 필요하지 않은 경우에 유용할 수 있습니다.

- AMS가 알림을 처리하고, 자동화를 실행하고, 필요한 경우 인시던트 사례를 생성하려면 기본값을 선택합니다.
4. 해결 시간: 24시간, 48시간 또는 72시간을 선택합니다. 마지막으로 인시던트 사례가 자동으로 종료되는 시점을 구성합니다. 마지막 사례 대응의 시간이 구성된 이후 해결 값에 도달하면 인시던트가 종료됩니다.

경고 알림

알림 처리의 일환으로 영향 분석을 기반으로 AWS Managed Services(AMS)는 인시던트를 생성하고 영향을 확인할 수 있는 문제 해결을 위한 인시던트 관리 프로세스를 시작합니다. 영향을 확인할 수 없는 경우 AMS는 서비스 알림을 통해 계정과 연결된 이메일 주소로 알림 알림을 보냅니다. 일부 시나리오에서는이 알림이 전송되지 않습니다. 예를 들어 인프라 관련 검사가 높은 CPU 사용률 알림을 통과하면 알림이 전송되지 않습니다. 자세한 내용은의 알림 처리 프로세스를 위한 AMS 모니터링 아키텍처 다이어그램을 참조하세요 [모니터링 작동 방식](#).

태그 기반 알림

태그를 사용하여 리소스에 대한 알림 알림을 다른 이메일 주소로 보냅니다. 여러 개발자 팀이 동일한 계정을 사용할 때 단일 이메일 주소로 전송된 알림으로 인해 혼동이 발생할 수 있으므로 태그 기반 알림은 사용하는 것이 가장 좋습니다. 태그 기반 알림은 선택한 [EC2 인스턴스 그룹화된 알림](#) 설정의 영향을 받지 않습니다.

태그 기반 알림으로 다음을 수행할 수 있습니다.

- 특정 이메일 주소로 알림 전송: `key = OwnerTeamEmail`,를 사용하여 특정 이메일 주소로 전송해야 하는 알림이 있는 리소스에 태그를 지정합니다 `value = EMAIL_ADDRESS`.
- 여러 이메일 주소로 알림 전송: 여러 이메일 주소를 사용하려면 쉼표로 구분된 값 목록을 지정합니다. 예, `key = OwnerTeamEmail`, `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ....` 값 필드의 총 문자 수는 260자를 초과할 수 없습니다.
- 사용자 지정 태그 키 사용: 사용자 지정 태그 키를 사용하려면 태그 기반 통신에 대한 자동 알림을 활성화하는 데 명시적으로 동의하는 이메일에 사용자 지정 태그 키 이름을 CSDM에 제공합니다. 모든 인스턴스와 리소스에서 고객 응대 태그에 동일한 태그 지정 전략을 사용하는 것이 가장 좋습니다.

Note

키 값 `OwnerTeamEmail`은 카멜 형식일 필요는 없습니다. 그러나 태그는 대/소문자를 구분하므로 권장 형식을 사용하는 것이 좋습니다.

이메일 주소는 도메인에서 로컬 부분을 분리하려면 "at sign"(@)을 사용하여 완전히 지정해야 합니다. 잘못된 이메일 주소의 예: *Team.AppATabc.xyz* 또는 *john.doe*. 태그 지정 전략에 대한 일반적인 지침은 [AWS 리소스 태그 지정](#)을 참조하세요. 태그에 개인 식별 정보(PII)를 추가하지 마세요. 가능하면 배포 목록 또는 별칭을 사용합니다.

태그 기반 알림은 EC2, Elastic Block Store(EBS), Elastic Load Balancing(ELB), Application Load Balancer(ALB), Network Load Balancer, Relational Database Service(RDS), OpenSearch, Elastic File System(EFS), FSx 및 Site-to-Site VPN과 같은 Amazon 서비스의 리소스에 대해 지원됩니다.

AMS 계정에 대한 모니터링 구성 보기

볼 수 있는 계정의 모니터링 구성에는 두 가지 주요 부분이 있습니다.

- CloudWatch 경보: CloudWatch 콘솔로 이동하여 다양한 관심 서비스를 선택하여 계정의 모든 CW 경보를 볼 수 있습니다.
- CloudWatch 이벤트:
 - 다중 계정 랜딩 영역: 계정에서 모니터링되는 CloudWatch 이벤트는 문자열이 인 모든 CW 이벤트 규칙을 필터링하여 찾을 수 있습니다"ams-".
 - 단일 계정 랜딩 영역: 계정에서 모니터링되는 CloudWatch 이벤트는 문자열이 인 모든 CW 이벤트 규칙을 필터링하여 찾을 수 있습니다"mc-".

AMS 계정에 대한 모니터링 구성 변경

Amazon EC2 리소스에 대한 기존 모니터링 구성을 변경할 수 있습니다. 구성할 수 있는 알림은 섹션을 참조하세요 [AMS의 기존 모니터링 알림](#). 알림이 애플리케이션의 운영 요구 사항을 충족하도록 기존 모니터링에 대한 경보 정의, 경보 대상 또는 경보 알림 옵트아웃을 변경할 수 있습니다. 다음 세부 정보와 함께 관리 | 기타 | 기타 | CT 업데이트(ct-0xdawir96cy7k)를 제출하여 앞서 언급한 변경 사항 중 일부 또는 전부를 요청할 수 있습니다.

- 인스턴스 IDs[선택 사항, 언급되지 않은 경우 계정의 모든 인스턴스가 범위 내에 있음]
- CloudWatch 지표 이름, 예: CPU 사용률/스왑 프리/IOwait
- 대상 - SMS/SNS 주제의 이메일 ID/전화 번호

기존 모니터링 구성에서 요청할 수 있는 변경 유형에 대한 자세한 내용은 [Amazon CloudWatch 설명서를](#) 참조하세요.

AMS의 애플리케이션 인식 인시던트 알림

애플리케이션 인식 자동 인시던트 알림을 사용하여 AMS가 사용자를 대신하여 생성하는 지원 사례에 맞게 통신 환경을 사용자 지정할 수 있습니다. 이 기능을 사용하면 AMS는 [AWS Service Catalog AppRegistry](#)에서 사용자 지정 워크로드 기본 설정을 검색하여 애플리케이션에 대한 메타데이터로 AMS 인시던트 통신을 보강하고 사용자를 대신하여 AMS에서 생성한 지원 사례의 심각도를 사용자 지정합니다. 이 기능을 사용하려면 먼저 AMS 계정에서 AWS Service Catalog AppRegistry를 프로비저닝해야 합니다.

AMS 모니터링 기본값에 대한 자세한 내용은 섹션을 참조하세요 [AMS의 모니터링 및 이벤트 관리](#).

AMS 계정에서 AppRegistry 프로비저닝 및 애플리케이션 생성

AppRegistry 서비스는 AMS 계정의 셀프 서비스 프로비저닝(SSP) 모드에서 사용할 수 있습니다. 액세스를 요청하는 방법에 대한 지침은 [AMS SSP를 사용하여 AMS 계정 AWS Service Catalog AppRegistry에서 프로비저닝을 참조하세요](#).

AppRegistry를 프로비저닝한 후 다음 방법 중 하나를 사용하여 애플리케이션을 생성합니다.

1. AWS 콘솔: AWS 콘솔을 통해 AppRegistry에서 애플리케이션을 생성하는 방법에 대한 자세한 내용은 AppRegistry 관리자 안내서의 [애플리케이션 생성](#)을 참조하세요. AWS Service Catalog AppRegistry
2. CloudFormation: 다른 리소스를 정의하는 것처럼 AppRegistry 애플리케이션을 정의할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 [AWS Service Catalog AppRegistry 리소스 유형 참조](#)를 참조하세요.

태그를 생성하여 사례 보강 활성화

AMS가 애플리케이션 메타데이터에 액세스하려면 먼저 애플리케이션에 태그를 지정해야 합니다. 다음 표에는 필수 태그가 나열되어 있습니다.

태그 키	태그 값
ams 관리형	true

애플리케이션에 대한 AMS 지원 사례 심각도 사용자 지정

애플리케이션이 조직에 얼마나 중요한지 지정하여 AMS에서 생성한 지원 사례의 심각도를 사용자 지정할 수 있습니다. 이 설정은 AppRegistry의 애플리케이션과 연결된 속성 그룹에 의해 제어됩니다. 속성 그룹 이름의 이름은 다음 패턴과 일치해야 합니다.

```
AMS.<ApplicationName>.CommunicationOptions
```

위의 패턴에서는 애플리케이션을 생성할 때 AppRegistry에 사용된 이름과 일치해야 ApplicationName 합니다.

예제 콘텐츠:

```
{
  "SchemaVersion": "1.0",
  "Criticality": "low"
}
```

SchemaVersion

이를 통해 사용 중인 스키마 버전과 사용할 수 있는 기능의 하위 집합이 결정됩니다.

스키마 버전	Feature
1.0	중요도 값에 따른 사용자 지정 지원 사례 심각도

중요도

이 애플리케이션의 중요도에 따라 AMS 자동 시스템에서 생성된 지원 사례의 심각도가 결정됩니다.

유효한 값:

```
low|normal|high|urgent|critical
```

심각도 수준에 대한 자세한 내용은 API 참조의 [SeverityLevel](#)을 참조하세요. AWS Support

필수 여부: 예

필요한 권한 검토

이 기능을 사용하려면 AMS가 다음 AWS Identity and Access Management 권한에 액세스해야 합니다.

- iam:ListRoleTags
- iam:ListUserTags
- resourcegroupstaggingapi:GetResources
- servicecatalog-appregistry:GetApplication
- servicecatalog-appregistry:ListAssociatedAttributeGroups
- servicecatalog-appregistry:GetAttributeGroup

Important

이전 작업을 거부하는 IAM 정책 또는 서비스 제어 정책(SCP)이 없는지 확인합니다.

API 호출은 `ams-access-admin` 역할에 의해 이루어집니다. 다음은 볼 수 있는 내용의 예입니다.

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSMetadataLookup-*
```

AMS에서 OpsCenter 사용

AWS Managed Services(AMS) 운영 팀은 [AWS Systems Manager OpsCenter](#)를 사용하여 리소스와 관련된 많은 알림을 진단하고 해결합니다.

OpsCenter를 사용하면 평균 해결 시간(MTTR)을 줄이는 동시에 AMS 운영 팀의 운영 대기열을 투명하게 볼 수 있습니다.

OpsCenter를 사용하면 AMS는 자동화된 솔루션 외에도 AMS 팀이 적극적으로 작업하는 [OpsItems](#)라고도 하는 운영 작업 항목을 투명하게 볼 수 있습니다.

OpsCenter 및 OpsItems. [AWS Systems Manager OpsCenter](#) AWS Management Console에 액세스하는 방법에 대한 자세한 내용은 [AWS Management Console 작업을 참조하세요](#). AWS 관리 콘솔에서 AWS Systems Manager 콘솔 및 OpsCenter로 이동할 수 있습니다. 자세한 내용은 [AWS Systems Manager 세션 관리자](#)를 참조하세요. OpsCenter는 사용할 수 있는 API도 제공합니다. 자세한 내용은 [OpsCenter에 대해 자세히 알아보기](#)를 참조하세요.

OpsCenter는 비용이 10 USD 미만인 약 1,000개의 OpsItems 포함된 가격 책정된 기능입니다. 자세한 내용은 [AWS Systems Manager 요금](#)을 참조하십시오.

AMS의 알림

알림 처리의 일환으로 영향 분석을 기반으로 AWS Managed Services(AMS)는 인시던트를 생성하고 영향을 확인할 수 있는 문제 해결을 위한 인시던트 관리 프로세스를 시작합니다. 영향을 확인할 수 없는 경우 AMS는 서비스 알림을 통해 계정과 연결된 이메일 주소로 알림 알림을 보냅니다.의 알림 처리 프로세스에 대한 AMS 모니터링 아키텍처 다이어그램을 참조하세요 [모니터링 작동 방식](#).

AMS에서 생성된 알림 수신

AWS Managed Services(AMS)를 사용하면 Amazon EC2 리소스에 대한 알림 알림을 직접 수신하여 통신 지연을 줄일 수 있습니다. Amazon EC2 알림을 직접 수신하려면 관리 | 모니터링 및 알림 | SNS | 변경 유형 구독(ct-3rc19u1k017wu)을 사용하여 대상(기본 이메일)에서 Amazon SNS 주제 Direct-Customer-Alerts를 구독합니다.

Note

모든 기존 알림이 기본적으로 Direct-Customer-Alerts 주제로 전송되는 것은 아닙니다. AMS 모니터링 시스템에서 생성되는 모든 알림을 보려면 AMS 모니터링 시스템에 대한 Amazon SNS 주제를 구독합니다. 요청에서 "AMS 모니터링 주제"를 요청하고, 알림을 수신할 구독 채널(Lambda, Amazon SQS, HTTP/S, 이메일 또는 SMS)을 지정하고, 알림을 수신할 엔드포인트(예: 이메일 프로토콜을 선택한 경우 이메일 주소)를 지정합니다. AMS 모니터링 주제는 AMS 공유 서비스에서 사용하는 알림을 수신하므로 노이즈가 발생할 수 있습니다.

자세한 내용은 Amazon Simple Notification Service [구독](#) API 참조의 구독 섹션을 참조하세요.

AMS가 제공하는 기존 알림 목록은 섹션을 참조하세요 [AMS의 기존 모니터링 알림](#).

AMS의 태그 기반 알림

태그를 사용하여 리소스에 대한 알림 알림을 다른 이메일 주소로 보냅니다. 여러 개발자 팀이 동일한 계정을 사용할 때 단일 이메일 주소로 전송된 알림으로 인해 혼동이 발생할 수 있으므로 태그 기반 알림은 사용하는 것이 가장 좋습니다.

⚠ Important

태그 기반 알림은 Amazon EC2, Amazon EBS, Elastic Load Balancing, Network Load Balancer, Application Load Balancer, Amazon RDS, Amazon Redshift 및 OpenSearch와 관련된 알림에만 작동합니다.

태그에 개인 식별 정보(PII)를 추가하지 마세요.

특정 이메일 주소로 알림 전송

key = OwnerTeamEmail,를 사용하여 특정 이메일 주소로 전송해야 하는 알림이 있는 리소스에 태그를 지정합니다value = **EMAIL_ADDRESS**.

여러 이메일 주소로 알림 전송

여러 이메일 주소를 사용하려면 쉼표로 구분된 값 목록을 지정합니다. 예, key = **OwnerTeamEmail**, value = **EMAIL_ADDRESS_1**, **EMAIL_ADDRESS_2**, **EMAIL_ADDRESS_3**, ... 값 필드의 총 문자 수는 260자를 초과할 수 없습니다.

사용자 지정 태그 키 사용

사용자 지정 태그 키를 사용하려면 태그 기반 통신에 대한 자동 알림을 활성화하는 데 동의하는 이메일에 사용자 지정 태그 키 이름을 CSDM에 제공합니다. 모든 인스턴스와 리소스에서 고객 응대 태그에 동일한 태그 지정 전략을 사용하는 것이 가장 좋습니다.

이메일 주소는 도메인에서 로컬 부분을 분리하려면 "at sign"(@)을 사용하여 완전히 지정해야 합니다. 잘못된 이메일 주소의 예: **Team.AppATabc.xyz** 또는 **john.doe**. 태그 지정 전략에 대한 일반적인 지침은 [태그 사용](#)을 참조하세요. 기존 리소스에 태그를 지정하려면 배포 | 고급 스택 구성 요소 | 태그 | 생성(자동)(ct-3cx7we852p3af) 변경 유형을 사용하여 RFC를 제출합니다.

i Note

키 값 **OwnerTeamEmail**은 카멜 형식일 필요는 없습니다. 그러나 태그는 대/소문자를 구분하므로 권장 형식을 사용하는 것이 좋습니다.

알림의 AMS 자동 문제 해결

확인 후 AWS Managed Services(AMS)는이 섹션에 설명된 특정 조건 및 프로세스에 따라 특정 알림을 자동으로 수정합니다.

알림 이름	설명	임계값	작업
보안 채널 끊김	인스턴스가 AD 도메인 컨트롤러와의 연결이 끊어지면 Windows EC2 인스턴스에서 보안 채널 경보가 트리거됩니다.	임계값이 지난 15분 동안 정의된 값을 10회 초과합니다.	AMS 자동 수정은 인스턴스가 SSM에서 온라인 상태이고 호스트 이름이 중복되지 않으며 AD 컴퓨터 객체가 CloudFormation 스택과 정렬되었는지 확인합니다. 수정 사항은 보안 채널 연결을 복구하여 인스턴스에 대한 액세스를 복원합니다.
상태 확인 실패	가능한 하드웨어 장애 또는 인스턴스의 장애 상태입니다.	시스템에서 지난 15분 이내에 한 번 이상 실패 상태를 감지했습니다.	AMS 자동 수정은 먼저 인스턴스에 액세스할 수 있는지 확인합니다. 인스턴스에 액세스할 수 없는 경우 인스턴스가 중지되고 다시 시작됩니다. 중지 및 시작을 사용하면 인스턴스가 새 기본 하드웨어로 마이그레이션할 수 있습니다. 자세한 내용은 “EC2 상태 확인 실패 수정 자동화” 섹션을 참조하세요.
AMSLinuxDiskUsage	EC2 인스턴스에서 1개의 탑재 지점(볼륨에 지정된 공간)의 디스크 사용량이 가득 차면 트리거됩니다.	임계값이 지난 30분 동안 정의된 값을 6회 초과합니다.	AMS 자동 수정은 먼저 임시 파일을 삭제합니다. 이렇게 해도 충분한 디스크 공간이 확보되지 않으면 볼륨이 가득 차면 가동 중지를 방지하기 위해 볼륨이 확장됩니다.
AMSWindowsDiskUsage	EC2 인스턴스에서 1개의 탑재 지점(볼륨에 지정된 공간)의 디스크 사용량이 가득 차면 트리거됩니다.	임계값이 지난 30분 동안 정의된 값을 6회 초과합니다.	AMS 자동 수정은 먼저 임시 파일을 삭제합니다. 이렇게 해도 충분한 디스크

알림 이름	설명	임계값	작업
	공간)의 디스크 사용량이 채워지는 경우.		공간이 확보되지 않으면 볼륨이 가득 차면 가동 중지를 방지하기 위해 볼륨이 확장됩니다.
RDS-EVENT-0089	DB 인스턴스가 할당된 스토리지의 90% 이상을 사용하였습니다.	스토리지가 90% 이상 할당되었습니다.	AMS 자동 수정은 먼저 DB가 수정 가능하고 사용 가능하거나 스토리지가 가득 찬 상태인지 확인합니다. 그런 다음 CloudFormation 변경 세트를 통해 할당된 스토리지, IOPS 및 스토리지 처리량을 늘리고 시도합니다. 스택 드리프트가 이미 감지된 경우 가동 중지 시간을 방지하기 위해 RDS API로 돌아갑니다. RDS DB 인스턴스에 다음 태그를 추가하여이 기능을 옵트아웃할 수 있습니다. "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

알림 이름	설명	임계값	작업
RDS-EVENT-0007	DB 인스턴스에 할당된 스토리지가 소진되었습니다. 해결하려면 추가 스토리지를 할당합니다.	스토리지는 100% 할당됩니다.	AMS 자동 수정은 먼저 DB가 수정 가능하고 사용 가능하거나 스토리지가 가득 찬 상태인지 확인합니다. 그런 다음 CloudFormation 변경 세트를 통해 할당된 스토리지, IOPS 및 스토리지 처리량을 늘리려고 시도합니다. 스택 드리프트가 이미 감지된 경우 가동 중지 시간을 방지하기 위해 RDS API로 돌아가집니다. RDS DB 인스턴스에 다음 태그를 추가하여이 기능을 옵트아웃할 수 있습니다. "Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".

알림 이름	설명	임계값	작업
RDS-EVENT-0224	요청된 할당된 스토리지가 구성된 최대 스토리지 임계값에 도달하거나 초과합니다.	DB 인스턴스의 최대 스토리지 임계값이 소진되었거나 요청된 할당된 스토리지보다 크거나 같습니다.	AMS 자동 수정은 먼저 요청된 양의 RDS 스토리지가 최대 스토리지 임계값을 위반하는지 확인합니다. 확인되면 AMS는 CloudFormation 변경 세트를 사용하여 최대 스토리지 임계값을 30% 늘리거나 CloudFormation을 통해 리소스가 프로비저닝되지 않은 경우 RDS API를 직접 늘리려고 시도합니다. RDS DB 인스턴스에 다음 태그를 추가하여이 기능을 옵트아웃할 수 있습니다. <pre>"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".</pre>

알림 이름	설명	임계값	작업
RDS-Storage-Capacity	DB 인스턴스에 할당된 스토리지에 1GB 미만이 남아 있습니다.	스토리지는 99% 할당됩니다.	AMS 자동 수정은 먼저 DB가 수정 가능하고 사용 가능하거나 스토리지가 가득 찬 상태인지 확인합니다. 그런 다음 CloudFormation 변경 세트를 통해 할당된 스토리지, IOPS 및 스토리지 처리량을 늘리려고 시도합니다. 스택 드리프트가 이미 감지된 경우 가동 중지 시간을 방지하기 위해 RDS API로 돌아가집니다. RDS DB 인스턴스에 다음 태그를 추가하여이 기능을 옵트아웃할 수 있습니다. "Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Amazon EC2 손상된 보안 채널: 문제 해결 자동화 참고 사항

AWS Managed Services(AMS) 자동 수정이 Amazon EC2 Windows 손상된 보안 채널 문제를 해결하기 전에 자동화는 다음과 같은 사전 확인을 수행하고 추가 조사를 위해 인시던트 보고서를 생성합니다.

- Amazon EC2 인스턴스 SSM 상태가 "온라인"인지 확인합니다.
- Amazon EC2 인스턴스가 Auto Scaling 그룹의 일부인지 여부와 Auto Scaling 그룹의 모든 인스턴스에 동일한 호스트 이름이 있는지 확인합니다.
- Amazon EC2 인스턴스가 프로비저닝에 사용된 CloudFormation 스택의 일부인지 확인합니다. 인스턴스가 CloudFormation 스택에서 제거된 경우 자동화는 연결된 Active Directory 조직 단위(OU)가 여전히 스택을 참조하고 있는지 확인합니다.

위의 검증이 통과되면 자동화가 중단된 보안 채널을 해결합니다.

문제 해결 단계:

- 자동 수정은 EC2 인스턴스와 AD 도메인 간의 보안 채널을 복구하여 인스턴스에 대한 액세스를 복원하려고 시도합니다.
- 문제 해결 후 자동화는 보안 채널이 설정되었는지 확인합니다. 실패한 경우 AMS는 인시던트를 생성하고 조사를 위해 AMS 작업을 참여시킵니다.

EC2 상태 확인 실패: 수정 자동화 참고 사항

AMS 자동 수정이 EC2 상태 확인 실패 문제와 작동하는 방식:

- Amazon EC2 인스턴스에 연결할 수 없는 경우 인스턴스를 중지했다가 다시 시작해야 새 하드웨어로 마이그레이션하고 복구할 수 있습니다.
- 문제의 루트가 OS(fstab에서 디바이스 누락, 커널 손상 등) 내에 있는 경우 자동화가 인스턴스를 복구할 수 없습니다.
- 인스턴스가 Auto Scaling 그룹에 속하는 경우 자동화는 아무 작업도 수행하지 않습니다. AutoScalingGroup 조정 작업은 인스턴스를 대체합니다.
- 인스턴스에 EC2 Auto Recovery가 활성화된 경우 문제 해결은 조치를 취하지 않습니다.

EC2 볼륨 사용량 수정 자동화

AWS Managed Services(AMS) 자동 수정이 EC2 볼륨 사용 문제와 작동하는 방식:

- 자동화는 먼저 볼륨 확장이 필요한지 여부와 수행할 수 있는지 확인합니다. 확장이 적절한 것으로 간주되는 경우 자동화를 통해 볼륨 용량을 늘릴 수 있습니다. 이 자동화된 프로세스는 성장의 필요성과 제어되고 제한된 확장의 균형을 맞춥니다.
- 볼륨을 확장하기 전에 자동화는 인스턴스에서 정리 작업(Windows: Disk Cleaner, Linux: Logrotate + Simple Service Manager 에이전트 로그 제거)을 수행하여 공간을 확보하려고 시도합니다.

Note

정리 작업은 지속적인 기능을 위해 CPU 크레딧에 의존하기 때문에 EC2 "T" 패밀리 인스턴스에서 실행되지 않습니다.

- Linux에서는 자동화가 EXT2, EXT3, EXT4 및 XFS 유형의 파일 시스템 확장만 지원합니다.

- Windows에서는 자동화가 NTFS(New Technology File System) 및 ReFS(Resilient File System)만 지원합니다.
- 자동화는 논리적 볼륨 관리자(LVM) 또는 RAID 배열의 일부인 볼륨을 확장하지 않습니다.
- 자동화는 인스턴스 스토어 볼륨을 확장하지 않습니다.
- 영향을 받는 볼륨이 이미 2TiB보다 큰 경우 자동화는 조치를 취하지 않습니다.
- 자동화를 통한 확장은 시스템 수명 주기 동안 일주일에 최대 3회, 총 5회로 제한됩니다.
- 이전 확장이 지난 6시간 이내에 발생한 경우 자동화는 볼륨을 확장하지 않습니다.

이러한 규칙으로 인해 자동화가 조치를 취하지 못하면 AMS는 아웃바운드 서비스 요청을 통해 사용자에게 연락하여 수행할 다음 조치를 결정합니다.

Amazon RDS 스토리지 부족 이벤트 수정 자동화

Amazon RDS 스토리지 부족 이벤트 문제에서 AWS Managed Services(AMS) 자동 수정이 작동하는 방식:

- Amazon RDS 인스턴스 스토리지를 확장하기 전에 자동화는 몇 가지 검사를 수행하여 Amazon RDS 인스턴스가 수정 가능하고 사용 가능한 상태인지 또는 스토리지 가득 참 상태인지 확인합니다.
- CloudFormation 스택 드리프트가 감지되면 Amazon RDS API를 통해 수정이 이루어집니다.
- 다음 시나리오에서는 문제 해결 작업이 실행되지 않습니다.
 - Amazon RDS 인스턴스 상태가 "사용 가능" 또는 "스토리지 가득 참"이 아닙니다.
 - Amazon RDS 인스턴스 스토리지는 현재 수정할 수 없습니다(예: 지난 6시간 동안 스토리지가 수정된 경우).
 - Amazon RDS 인스턴스에 오토 스케일링 스토리지가 활성화되어 있습니다.
 - Amazon RDS 인스턴스는 CloudFormation 스택 내의 리소스가 아닙니다.
- 문제 해결은 6시간당 1회 확장으로 제한되며 14일 동안 최대 3회 확장으로 제한됩니다.
- 이러한 시나리오가 발생하면 AMS는 아웃바운드 인시던트를 통해 사용자에게 연락하여 다음 조치를 결정합니다.

AMS에서 추가 CloudWatch 경보 생성

AWS Managed Services(AMS) 배포 | 모니터링 및 알림 | CloudWatch | 경보 변경 유형 생성을 사용하여 새 CloudWatch 경보를 생성할 수 있습니다.

⚠ Important

AMS는 사용자가 생성한 CloudWatch 경보를 모니터링하지 않습니다.

Amazon EC2 인스턴스에 대한 사용자 지정 CloudWatch 지표 및 경보 사용(Auto Scaling 그룹에 배포된 업데이트된 AMIs에 의존하지 않는 변경 가능한 배포에만 작동):

1. 애플리케이션 모니터링 스크립트와 사용자 지정 지표를 생성합니다. 예제 스크립트에 대한 자세한 내용과 액세스는 [Amazon EC2 Linux 인스턴스의 메모리 및 디스크 지표 모니터링을 참조하세요](#). Linux Amazon EC2 인스턴스용 Amazon CloudWatch 모니터링 스크립트는 Amazon CloudWatch 사용자 지정 지표를 생성하고 사용하는 방법을 보여줍니다. Amazon EC2 이 예제는 Linux 인스턴스에 대한 메모리, 스왑 및 디스크 공간 사용을 측정치를 보고하는 완벽하게 작동하는 예로 구성된 Perl 스크립트입니다.
2. 모니터링 스크립트를 업로드합니다. 모니터링 스크립트를 Auto Scaling 그룹 또는 Amazon EC2 인스턴스 구성에 업로드하려면 Auto Scaling 그룹 또는 Amazon EC2 인스턴스를 구성할 때 UserData를 사용하거나, 애플리케이션이 CodeDeploy와 함께 배포된 경우 배포 | 애플리케이션 | CodeDeploy 애플리케이션 | CT 배포(ct-2edc3sd1™rb)를 사용하여 구성을 수정할 수 있습니다.
3. 사용자 지정 지표를 CloudWatch에 게시합니다(새 사용자 지정 지표에 대한 데이터 포인트를 처음 게시할 때 생성됨). [사용자 지정 지표 게시를 참조하세요](#).
4. CloudWatch 경보를 생성[하려면 인스턴스에 대한 CloudWatch 경보 생성을 참조하세요](#).

⚠ Important

모니터링 데이터가 경로 [infra/INSTANCE_ID/YOUR_CUSTOM_METRIC]로 전송해야 합니다.

CloudWatch 경보를 수정하거나 삭제하려면 Amazon CloudWatch API 참조 [PutMetricAlarm](#)에 설명된 대로 작업을 완료하는 데 필요한 파라미터와 함께 관리 | 기타 | 기타 | 변경 유형 생성(ct-1e1xtak34nx76)을 사용하여 RFC를 제출합니다.

CloudWatch 이벤트 스트림을 사용할 수 있습니다. AMS는 CloudWatch와 통합되며 모든 AWS API 호출이 CloudWatch 이벤트를 트리거하도록 요청할 수 있습니다.

이렇게 하려면 관심 있는 API 직접 호출로 관리 | 기타 | 기타 | CT 업데이트(ct-0xdawir96cy7k)를 제출합니다. AMS 운영자가 요구 사항을 수집하기 위해 연락을 드릴 것입니다. 자세한 내용은 [Amazon CloudWatch 설명서를](#) 참조하세요.

CloudWatch 이벤트 스트림에 액세스하려면 관리 | 기타 | 기타 | CT 업데이트(ct-0xdawir96cy7k)를 제출하여 SNS 알림 주제에 당사자를 추가합니다. AMS 운영자가 요구 사항을 수집하기 위해 연락을 드릴 것입니다.

AMS에서 사용자 지정 CloudWatch 지표 및 경고 생성

비즈니스 및 애플리케이션 지표를 Amazon CloudWatch에 저장할 수 있습니다. CloudWatch가 AWS Managed Services(AMS) 리소스에 대해 이미 저장한 지표와 마찬가지로 그래프를 보고 이러한 지표를 기반으로 경보를 설정할 수 있습니다. CloudWatch에 대한 자세한 내용은 [Amazon CloudWatch 개념을](#) 참조하세요.

Amazon SNS를 사용하면 애플리케이션이 경보가 게시되는 AMS Managed Monitoring System 또는 MMS, Amazon SNS(SNS) 주제, 이 경우 MMS 및 SQS 대기열에 대해 "푸시" 메커니즘을 통해 여러 구독자에게 중요한 메시지를 보낼 수 있습니다. CloudWatch를 사용하여 사용자 지정 지표를 생성하고 SNS 주제를 통해 AMS 경보를 적절하게 설정할 수 있습니다. 이를 수행하려면 다음 단계를 따릅니다.

Note

이 프로세스는 Auto Scaling 그룹에 배포된 업데이트된 AMIs에 의존하는 변경 불가능한 배포에는 작동하지 않으며 변경 가능한 애플리케이션(ASG 아님) 배포에 적합합니다. AMS Advanced의 제한 내에서 사용자 지정 지표를 설정하는 것은 복잡한 작업입니다. CloudWatch의 예제는 [예제: 용어 발생 횟수를 참조하세요](#).

1. 애플리케이션 모니터링 스크립트와 사용자 지정 지표(예: 발생 횟수 예제)를 생성합니다. 예제 스크립트에 대한 자세한 내용과 액세스는 [Amazon EC2 Linux 인스턴스의 메모리 및 디스크 지표 모니터링을 참조하세요](#).
2. 모니터링 스크립트를 업로드합니다. Auto Scaling 그룹 또는 Amazon EC2 인스턴스 구성에 모니터링 스크립트를 업로드하려면 Auto Scaling 그룹 또는 Amazon EC2 인스턴스를 구성할 때 UserData를 사용하거나, 애플리케이션이 CodeDeploy와 함께 배포된 경우 Deployment | Applications | CodeDeploy application | Deploy CT(ct-2edc3sd1™rb)를 사용하여 구성을 수정할 수 있습니다.
3. 사용자 지정 지표를 CloudWatch에 게시합니다(새 사용자 지정 지표에 대한 데이터 포인트를 처음 게시할 때 생성됨). [사용자 지정 지표 게시를 참조하세요](#).

4. 고객 지표를 애플리케이션 모니터링 시스템에 통합하려면 AMS에 배포 | 모니터링 및 알림 | SNS | 변경 유형 생성(ct-3dfnglm4ombbs)이 포함된 RFC를 제출하여 지표에 대한 SNS 주제 생성을 요청합니다.
5. CloudWatch 경보를 생성하려면 [Amazon CloudWatch 경보 생성을 참조하세요](#).

⚠ Important

모니터링 데이터는 [infra/**INSTANCE_ID/YOUR_CUSTOM_METRIC**] 경로로 전송해야 합니다.

AMS에서 .Net 및 SQL Server용 CloudWatch Application Insights 사용

Amazon CloudWatch Application Insights를 사용하여 AWS Managed Services(AMS) 애플리케이션 리소스에 대한 모니터를 설정하여 데이터에 애플리케이션 문제의 징후가 있는지 지속적으로 분석하고 애플리케이션 문제를 해결할 때 평균 복구 시간(MTTR)을 줄일 수 있습니다. CloudWatch Application Insights에 대한 자세한 내용은 [.NET 및 SQL Server용 CloudWatch Application Insights](#)를 참조하세요.

⚠ Important

AMS는 사용자가 제어하는 애플리케이션 코드를 위한 문제이므로 CloudWatch Application Insights의 문제를 모니터링하지 않습니다.

CloudWatch Application Insights를 사용하려면 배포 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 개체 또는 정책 생성(검토 필요) 변경 유형(ct-3dpd8mdd9jn1r)이 포함된 RFC를 CloudWatch Application Insights를 구성할 수 있는 권한을 제공하는 IAM 역할을 생성하라는 요청과 함께 제출합니다. 식별된 문제를 수신하려면 SNS 주제를 통해 또는 CloudWatch 이벤트 규칙의 대상과 함께 두 가지 옵션이 있습니다. RFC에서 원하는 항목을 지정합니다. CloudWatch 이벤트 규칙을 사용하려는 경우 RFC에서 규칙 정의도 지정합니다. CloudWatch Application Insights를 설정하면 가능한 근본 원인을 가리키는 인사이트를 포함하여 잠재적 문제에 대한 알림을 받게 됩니다.

역할을 수임하는 방법을 알아보려면 AMS 온보딩 가이드에서 [Active Directory를 AMS IAM 역할과 연동을 참조하세요](#).

AMS에서 Amazon EventBridge 관리형 규칙 사용

AMS Advanced는 Amazon EventBridge 관리형 규칙을 사용합니다. 관리형 규칙은 AMS에 직접 연결된 고유한 유형의 규칙입니다. 이러한 규칙은 수신 이벤트를 일치시키고 처리를 위해 대상으로 전송합니다. 관리형 규칙은 AMS에서 사전 정의하며 서비스에서 고객 계정을 관리하는 데 필요한 이벤트 패턴을 포함합니다. 달리 정의되지 않은 한 소유 서비스만 이러한 관리형 규칙을 활용할 수 있습니다.

AMS 관리형 규칙은 `events.managedservices.amazonaws.com` 서비스 보안 주체에 연결됩니다. 이러한 관리형 규칙은 [AWSServiceRoleForManagedServices_Events 서비스 연결 역할을](#) 통해 관리됩니다. 이러한 규칙을 삭제하려면 고객의 특별한 확인이 필요합니다. 자세한 내용은 [AMS에 대한 관리형 규칙 삭제를 참조하세요](#).

규칙에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 [규칙을](#) 참조하세요.

AMS에서 배포한 Amazon EventBridge 관리형 규칙

Amazon EventBridge 관리형 규칙

규칙 이름	설명	정의
AMSAdvancedCoreRule	이 규칙은 Amazon CloudWatch 경보를 AMS 모니터링으로 전달합니다. Amazon CloudWatch 이벤트는 CloudWatch 경보를 모니터링합니다.	<pre>{ { "source": ["aws.cloudwatch"], "detail-type": ["CloudWatch Alarm State Change"], } }</pre>

AMS에 대한 관리형 규칙 생성

Amazon EventBridge 관리형 규칙을 수동으로 생성할 필요가 없습니다. AWS 관리 콘솔 AWS CLI, 또는 AWS API에서 AMS에 온보딩하면 AMS가 자동으로 AMS를 생성합니다.

AMS에 대한 관리형 규칙 편집

AMS에서는 관리형 규칙을 편집할 수 없습니다. 각 관리형 규칙의 이름 및 이벤트 패턴은 AMS에서 사전 정의됩니다.

AMS에 대한 관리형 규칙 삭제

관리형 규칙을 수동으로 삭제할 필요가 없습니다. AWS 관리 콘솔, AWS CLI 또는 AWS API의 AMS에서 오프보드하면 AMS가 리소스를 정리하고 AMS가 소유한 모든 관리형 규칙을 삭제합니다.

AMS가 오프보딩 중에 관리형 규칙을 제거하지 못하는 경우 Amazon EventBridge 콘솔, AWS CLI 또는 AWS API를 사용하여 관리형 규칙을 수동으로 삭제할 수도 있습니다. 이렇게 하려면 먼저 AMS에서 오프보드하고 관리형 규칙을 강제로 삭제해야 합니다.

AMS의 신뢰할 수 있는 수정자

Trusted Remediator는 [AWS Trusted Advisor](#) 및 [AWS Compute Optimizer](#) 권장 사항의 문제 해결을 자동화하는 AWS Managed Services 솔루션입니다. Trusted Remediator는 Trusted Advisor 및 Compute Optimizer가 비용을 절감하거나, 시스템 가용성을 개선하거나, 성능을 최적화하거나,의 보안 격차를 줄일 수 있는 기회를 나타낼 때 권장 사항을 생성합니다 AWS 계정. Trusted Remediator를 사용하면 확립된 모범 사례를 사용하는 안전하고 표준화된 방식으로 이러한 보안, 성능, 비용 최적화, 내결함성 및 서비스 제한 권장 사항을 해결할 수 있습니다. Trusted Remediator를 사용하면 문제 해결 솔루션을 구성할 수 있으며 생성한 일정에 따라 자동으로 실행되므로 문제 해결 프로세스가 간소화됩니다. 이 간소화된 접근 방식은 수동 개입 없이 일관되고 효율적으로 문제를 해결합니다.

신뢰할 수 있는 교정기 주요 이점

다음은 Trusted Remediator의 주요 이점입니다.

- 보안, 성능 및 비용 최적화 개선: Trusted Remediator를 사용하면 계정의 전반적인 보안 태세를 강화하고, 리소스 사용률을 최적화하고, 운영 비용을 절감할 수 있습니다.
- 셀프 서비스 설정 및 구성: 요구 사항 및 기본 설정에 맞게 신뢰할 수 있는 교정기를 구성할 수 있습니다.
- 자동 Trusted Advisor 검사 및 AWS Compute Optimizer 권장 사항 수정: 구성 후 신뢰할 수 있는 수정자는 선택한 검사에 대한 수정 작업을 자동으로 실행합니다. 이 자동화를 사용하면 수동 개입이 필요하지 않습니다.
- 모범 사례 구현: 해결 작업은 확립된 모범 사례를 기반으로 하므로 표준화되고 효과적인 방식으로 문제를 해결합니다.

- 예약된 실행: day-to-day 운영 워크플로에 맞는 수정 일정을 선택할 수 있습니다.

Trusted Remediator를 사용하면 AWS 환경에서 식별된 문제를 사전에 해결할 수 있으므로 모범 사례를 준수하고 안전하고 성능이 뛰어나며 비용 효율적인 클라우드 인프라를 유지할 수 있습니다.

신뢰할 수 있는 수정자 작동 방식

다음은 신뢰할 수 있는 수정자 워크플로의 그림입니다.

Trusted Remediator는 Trusted Advisor에 대한 Compute Optimizer 권장 사항을 평가하고 OpsCenter에서 [OpsItems](#)를 AWS 계정 생성합니다 AWS Systems Manager . OpsCenter 그런 다음 Trusted Remediator 자동화 문서를 사용하여 OpsItems를 자동으로 또는 수동으로 수정할 수 있습니다. 다음은 각 문제 해결 유형에 대한 세부 정보입니다.

- 자동 수정: 신뢰할 수 있는 수정자가 자동화 문서를 실행하고 실행을 모니터링합니다. 자동화 문서가 완료되면 Trusted Remediator가 Opsitem을 해결합니다.
- 수동 수정: 신뢰할 수 있는 수정자는 검토할 수 있도록 OpsItem을 생성합니다. 검토 후 자동화된 RFC, [신뢰할 수 있는 수정자 | 조사 결과 | 수정](#), 변경 유형을 생성하여 리소스를 수정할 수 있습니다. 수동 문제 해결 단계에 대한 자세한 내용은 섹션을 참조하세요 [신뢰할 수 있는 수정자에서 수동 수정 실행](#).

수정 로그는 Amazon S3 버킷에 저장됩니다. S3 버킷의 데이터를 사용하여 보고를 위한 사용자 지정 QuickSight 대시보드를 구축할 수 있습니다. 또한 AMS는 신뢰할 수 있는 수정자에 대한 요청 시 보고서를 제공합니다. 이러한 보고서를 받으려면 CSDM에 문의하십시오.

신뢰할 수 있는 문제 해결사의 주요 용어

다음은 AMS에서 신뢰할 수 있는 교정기를 사용할 때 알아두는 데 유용한 용어입니다.

- AWS Trusted Advisor 및 AWS Compute Optimizer: AWS에서 제공하는 클라우드 최적화 서비스. Trusted Advisor 및 Compute Optimizer는 AWS 환경을 검사하고 다음 6가지 범주의 모범 사례를 기반으로 권장 사항을 제공합니다.
 - 비용 최적화
 - 성능
 - [Security]
 - 내결함성

- 운영 우수성
- 서비스 한도

자세한 내용은 [AWS Trusted Advisor](#) 및 [AWS Compute Optimizer](#) 섹션을 참조하세요.

- 신뢰할 수 있는 해결사: [Trusted Advisor](#) 검사 및 [AWS Compute Optimizer](#) 권장 사항을 위한 AMS 문제 해결 솔루션입니다. Trusted Remediator를 사용하면 알려진 모범 사례를 통해 Trusted Advisor 검사 및 Compute Optimizer 권장 사항을 안전하게 해결하여 보안, 성능을 개선하고 비용을 절감할 수 있습니다. Trusted Remediator는 쉽게 설정하고 구성할 수 있습니다. 를 한 번 구성하면 Trusted Remediator가 원하는 일정(매일 또는 매주)에 따라 문제 해결을 실행합니다.
- AWS Systems Manager SSM 문서:가 AWS 리소스에서 AWS Systems Manager 수행하는 작업을 정의하는 JSON 또는 YAML 파일입니다. SSM 문서는 여러 AWS 리소스 및 인스턴스에서 운영 작업을 자동화하는 선언적 사양 역할을 합니다.
- AWS Systems Manager OpsCenter OpsItem: 환경의 운영 문제를 추적하고 해결하는 데 도움이 되는 클라우드 운영 문제 관리 리소스입니다 AWS . OpsItems는 AWS 서비스 및 리소스 전반의 운영 데이터 및 문제에 대한 중앙 집중식 보기 및 관리 시스템을 제공합니다. 각 OpsItem은 잠재적 보안 위험, 성능 문제 또는 운영 인시던트와 같은 운영 문제를 나타냅니다.
- 구성: 구성은의 [AWS AppConfig기능인에 저장된 속성 집합입니다 AWS Systems Manager](#). 의 Trusted Remediator 애플리케이션은 계정 수준에서 문제 해결을 구성하는 데 AWS AppConfig 도움이 됩니다.
- 실행 모드: 실행 모드는 각 Trusted Advisor 검사 결과에 대해 문제 해결을 실행하는 방법을 결정하는 구성 속성입니다. 자동, 수동, 조건부, 비활성의 네 가지 실행 모드가 지원됩니다.
- 리소스 재정의:이 기능은 리소스 태그를 사용하여 특정 리소스에 대한 구성을 재정의합니다.
- 수정 항목 로그: 신뢰할 수 있는 수정자 수정 S3 로그 버킷의 로그 파일입니다. 문제 해결 항목 로그는 문제 해결 OpsItems 생성될 때 생성됩니다. 이 로그 파일에는 수동 실행 수정 OpsItems 및 자동 실행 수정 OpsItems. 이 로그 파일을 사용하여 모든 문제 해결 항목을 추적합니다.
- 자동 문제 해결 실행 로그: Trusted Remediator 문제 해결 S3 로그 버킷의 로그 파일입니다. SSM 문서 자동 실행이 완료되면 자동 문제 해결 실행 로그가 생성됩니다. 이 로그에는 자동 실행 문제 해결 OpsItems. 이 로그 파일을 사용하여 자동 문제 해결을 추적합니다.

AMS에서 신뢰할 수 있는 문제 해결사 시작하기

신뢰할 수 있는 수정자는 추가 비용 없이 AMS에서 사용할 수 있습니다. Trusted Remediator는 단일 계정 및 다중 계정 구성을 지원합니다.

신뢰할 수 있는 해결사에 온보딩

AMS 계정을 Trusted Remediator에 온보딩하려면 Cloud Architects 또는 Cloud Service Delivery Manager(CSDMs에 이메일을 보냅니다. 이메일 본문에 다음 정보를 포함합니다.

- AWS 계정: 12자리 계정 식별 번호입니다. 신뢰할 수 있는 해결자에게 온보딩하려는 모든 계정은 동일한 AMS Advanced 고객에게 속해야 합니다.
- 위임된 관리자 계정: Trusted Advisor 및 Compute Optimizer가 단일 또는 여러 계정에 대한 구성을 확인하는 데 사용되는 계정입니다.
- 멤버 계정: 위임된 관리자 계정에 연결된 계정입니다. 이러한 계정은 위임된 관리자 계정에서 구성을 상속합니다. 하나의 멤버 계정 또는 여러 개의 멤버 계정을 가질 수 있습니다.

Note

멤버 계정은 위임된 관리자 계정에서 구성을 상속합니다. 특정 계정에 대해 다른 구성이 필요한 경우 원하는 구성으로 여러 위임된 관리자 계정을 온보딩합니다. 온보딩하기 전에 Cloud Architects와 함께 계정 구조와 구성을 계획합니다.

- AWS 리전: 리소스가 AWS 리전 있는 입니다. 목록은 [AWS 서비스 리전별](#) 단원을 AWS 리전참조하십시오.
- 문제 해결 일정 및 시간: 선호하는 문제 해결 일정(일별 또는 주별). Trusted Remediator는 Trusted Advisor 검사를 수집하고 예약된 시간에 문제 해결을 시작합니다. 예를 들어 매주 일요일 오전 1시에 대한 수정 일정을 호주 동부 표준시로 설정할 수 있습니다.
- 알림 이메일: Trusted Remediator는 알림 이메일을 사용하여 문제 해결 시 매일 사용자에게 알립니다. 알림 이메일 제목은 "신뢰할 수 있는 해결 방법 수정 요약"이며 콘텐츠는 지난 24시간 동안 실행된 신뢰할 수 있는 해결 방법에 대한 정보를 제공합니다.

Note

예약된 모든 문제 해결 후 애플리케이션과 리소스를 검토합니다. 추가 지원이 필요한 경우 AMS에 문의하십시오.

필수 세부 정보가 포함된 온보딩 요청을 CA 또는 CSDM에 제출하면 AMS가 신뢰할 수 있는 해결자에게 계정을 온보딩합니다. Trusted Remediator는의 기능 AWS AppConfig인 AWS Systems Manager를 사용하여 Trusted Advisor 검사에 대한 구성을 정의합니다. 이러한 구성은에 저장된 속성 집합입니다 AWS AppConfig. 리소스에 대한 무단 요금을 방지하기 위해 계정이 신뢰할 수 있는 해결자에게 온보딩

되면 지원되는 모든 Trusted Advisor 검사가 비활성으로 설정됩니다. 이러한 구성을 통해 특정 Trusted Advisor 검사를 자동으로 수정하거나 나머지 검사를 평가하고 수동으로 수정할 수 있습니다. 구성은 사용자 지정이 가능하므로 각 Trusted Advisor 검사에 구성을 적용할 수 있습니다. 자세한 내용은 [신뢰할 수 있는 수정자에서 Trusted Advisor 검사 수정 구성](#) 단원을 참조하십시오.

에서 신뢰할 수 있는 수정자 구성 AWS 계정

온보딩이 완료되면 CA 또는 CDSM이 사용자에게 알리고 위임된 관리자에 기본 구성이 생성됩니다 AWS 계정. 구성은 Trusted Remediator 애플리케이션의 AWS AppConfig에 저장됩니다. RFC [관리 | 신뢰할 수 있는 수정자 | 수정 구성 | 업데이트](#)를 사용하여 구성 업데이트를 요청할 수 있습니다. 자세한 내용은 [신뢰할 수 있는 수정자에서 Trusted Advisor 검사 수정 구성](#) 단원을 참조하십시오.

기본 신뢰할 수 있는 수정자 구성을 보려면 다음 단계를 완료하세요.

1. <https://console.aws.amazon.com/systems-manager/> AWS Systems Manager 콘솔을 엽니다.

Note

위임된 관리자 계정에 있는지 확인합니다.

2. 애플리케이션 관리, AppConfig를 선택합니다.
3. 애플리케이션 목록에서 신뢰할 수 있는 수정자를 선택합니다.

다음은 신뢰할 수 있는 수정자 구성을 보여주는 AWS AppConfig 콘솔의 예입니다.

수정할 검사 및 권장 사항 선택

기본적으로 수정 실행 모드는 구성의 모든 Trusted Advisor 검사 및 Compute Optimizer 권장 사항에 대해 비활성입니다. 이렇게 하면 무단 수정을 방지하고 리소스를 보호할 수 있습니다. AMS는 Trusted Advisor 검사 문제 해결을 위해 선별된 SSM 자동화 문서를 제공합니다.

신뢰할 수 있는 수정자를 사용하여 수정하려는 검사를 선택하려면 다음 단계를 완료하세요.

1. 지원되는 [Trusted Advisor 및 Compute Optimizer 권장 사항의 목록 또는 관련 SSM 자동화 문서의 이름을](#) 검토하여 신뢰할 수 있는 문제 해결자를 통해 해결하려는 점검 및 권장 사항을 결정합니다.
2. [관리 제출 | 신뢰할 수 있는 수정자 | 수정 구성 | 선택한 검사에 대한 구성을 업데이트하도록](#) 요청 업데이트. Trusted Advisor 검사를 선택하는 방법에 대한 지침은 섹션을 참조하세요 [신뢰할 수 있는 수정자에서 Trusted Advisor 검사 수정 구성](#).

신뢰할 수 있는 수정자에서 수정 사항 추적

계정 수준 구성을 업데이트한 후 신뢰할 수 있는 수정자는 각 수정에 대해 OpsItems 생성합니다. Trusted Remediator는 문제 해결 일정에 따라 OpsItems의 자동 문제 해결을 위해 SSM 문서를 실행합니다. Systems Manager OpsItems 보는 방법에 대한 지침은 [섹션을 참조하세요](#) [신뢰할 수 있는 해결 방법에서 문제 해결 추적](#). OpsCenter

신뢰할 수 있는 수정자에서 수동 수정 실행

자동 RFC를 사용하여 Trusted Advisor 검사를 수동으로 수정할 수 있습니다. 수동 수정을 선택하면 신뢰할 수 있는 수정자가 수동 실행 OpsItem을 생성합니다. 자세한 내용은 [신뢰할 수 있는 수정자에서 수동 수정 실행](#) 단원을 참조하십시오.

Trusted Remediator에서 지원하는 Compute Optimizer 권장 사항

다음 표에는 지원되는 Compute Optimizer 권장 사항, SSM 자동화 문서, 사전 구성된 파라미터 및 자동화 문서의 예상 결과가 나열되어 있습니다. 검사 문제 해결을 위해 SSM 자동화 문서를 활성화하기 전에 예상 결과를 검토하여 비즈니스 요구 사항에 따라 가능한 위험을 이해하는 데 도움이 됩니다.

문제 해결을 활성화하려는 지원되는 검사에 대해 각 Compute Optimizer 검사에 해당하는 구성 규칙이 있는지 확인합니다. 자세한 내용은 [Trusted Advisor 검사 옵트인을 참조 AWS Compute Optimizer 하세요](#).

최적화 옵션	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
규모 조정		
Amazon EC2 인스턴스 권장 사항	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation Compute Optimizer 권장 사항에 따라 Amazon EC2 인스턴스 유형이 업데이트되었습니다. 옵션이 있는 경우 동일한 플랫폼 파라미터(아키텍처, 하이퍼바이저, 네트워크 인터페이스, 가상화 유형 등)를 유지하면서 가장 최적의 옵션을 선택합니다.	- MinimumDaysSinceLastChange: 마지막 인스턴스 유형 변경 이후 최소 일수를 지정하는 파라미터입니다. 기본값은 7일입니다. - 제한 조건 없음 - CreateAMIBeforeResize: 크기를 조정하기 전에 인스턴스 AMI를 백업으로 생성하려면 'True'로 설정합니다. 백업을 생성하지 않으려면

최적화 옵션	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		를 'False'로 설정합니다. 기본값은 'True'입니다. 제약 조건 없음

최적화 옵션	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Amazon EBS 볼륨 권장 사항	AWSManagedServices-ModifyEBSVolume Amazon EBS 볼륨은 Compute Optimizer 권장 사항에 따라 수정됩니다. 수정에는 볼륨 유형, 크기, IOPS, 볼륨 생성(gp2, gp3 등)이 포함될 수 있습니다.	• CreateSnapshot: 볼륨을 수정하기 전에 스냅샷을 생성하려면 'True'로 설정합니다. 스냅샷을 생성하지 않으려면 'False'로 설정합니다. 기본값은 'True'입니다. - 제약 조건 없음 • VolumeType: 원하는 볼륨 유형입니다. 유형을 지정하지 않으면 기존 유형이 유지됩니다. - 제약 조건 없음 • VolumeSize: 원하는 볼륨 크기로, GiB 단위입니다. 대상 볼륨 크기는 볼륨의 기존 크기보다 크거나 같아야 합니다. 크기를 지정하지 않으면 기존 크기가 유지됩니다. - 제약 조건 없음 • Iops: 요청된 초당 I/O 작업 수 (IOPS). 이 파라미터는 io1, io2 및 gp3 볼륨에만 유효합니다. - 제약 조건 없음 • 처리량: 볼륨에 프로비저닝할 처리량으로, 최대 1,000MiB/s입니다. 이 파라미터는 gp3 볼륨에만 유효합니다. - 제약 조건 없음 • RemediateStackDrift: 드리프트 수정을 시작하려면 볼륨 수정으로 인해 드리프트가 발생하는 경우 'True'로 설정합니다. 드리프트 수정

최적화 옵션	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		을 시도하지 않으려면들 'False'로 설정합니다. 기본값은 'True'입니다.
		제약 조건 없음
Lambda 함수 권장 사항	AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory AWS Lambda Compute Optimizer 권장 사항에 따라 함수 메모리 최적화.	RecommendedMemorySize: 권장 옵션과 다른 경우 사용자 지정 메모리 크기입니다. 제약 조건 없음
유휴 리소스		
유휴 Amazon EBS 볼륨	AWSManagedServices-DeleteUnusedEBSVolume 연결되지 않은 Amazon EBS 볼륨이 삭제됩니다.	• CreateSnapshot: 볼륨을 삭제하기 전에 스냅샷을 생성하려면들 'True'로 설정합니다. 스냅샷을 생성하지 않으려면들 'False'로 설정합니다. 기본값은 'True'입니다. 제약 조건 없음 • MinimumUnattachedDays: 삭제할 Amazon EBS 볼륨의 연결되지 않은 최소 일수, 최대 62일. 기본값은 7입니다. 제약 조건 없음
유휴 Amazon EC2 인스턴스	AWSManagedServices-StopEC2Instance 유휴 Amazon EC2 인스턴스가 중지됩니다.	ForceStopWithInstanceStore: 인스턴스 스토어를 사용하는 인스턴스에 대해 강제로 중지하려면들 'True'로 설정합니다. 강제 중지하지 않으려면들 'False'로 설정합니다. 기본값 'False'는 인스턴스 중지를 방지합니다. 제약 조건 없음

최적화 옵션	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
유휴 Amazon RDS 인스턴스	AWSManagedServices-StopIdleRDSInstance 유휴 Amazon RDS 인스턴스를 중지합니다. 지원되는 엔진은 MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL입니다. 이 문서는 Aurora MySQL 및 Aurora PostgreSQL에는 적용되지 않습니다. 인스턴스는 최대 7일까지 중지되고 자동으로 다시 시작됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

Trusted Advisor Trusted Remediator에서 지원하는 검사

다음 표에는 지원되는 Trusted Advisor 검사, SSM 자동화 문서, 사전 구성된 파라미터 및 자동화 문서의 예상 결과가 나와 있습니다. 검사 문제 해결을 위해 SSM 자동화 문서를 활성화하기 전에 예상 결과를 검토하여 비즈니스 요구 사항에 따라 가능한 위험을 이해하는 데 도움이 됩니다.

문제 해결을 활성화하려는 지원되는 Trusted Advisor 검사에 대해 각 검사에 해당하는 구성 규칙이 있는지 확인합니다. 자세한 내용은 [기반 AWS Trusted Advisor 검사 보기를 참조하세요 AWS Config](#). 점검에 해당 AWS Security Hub 제어가 있는 경우 Security Hub 제어가 활성화되어 있는지 확인합니다. 자세한 내용은 [Security Hub에서 제어 활성화](#)를 참조하세요. 미리 구성된 파라미터 관리에 대한 자세한 내용은 [Trusted Remediator의 Configure Trusted Advisor check remediation를 참조하세요](#).

Trusted Advisor Trusted Remediator에서 지원하는 비용 최적화 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Z4AUBRNSmz	AWSManagedServices-TrustedRemediatorReleaseElasticIP	사전 구성된 파라미터는 허용되지 않습니다.
연결되지 않은 탄력적 IP 주소	리소스와 연결되지 않은 탄력적 IP 주소를 해제합니다.	제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c18d2gz150 - Amazon EC2 인스턴스 중지됨	AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - 일 수 동안 중지된 Amazon EC2 인스턴스가 종료됩니다.	• CreateAMIBeforeTermination: Amazon EC2 인스턴스를 종료하기 전에 인스턴스 AMI를 백업으로 생성하려면를 선택합니다true. 종료하기 전에 백업을 생성하지 않으려면를 선택합니다false. 기본값은 true입니다. • AllowedDays: 인스턴스가 종료되기 전에 중지된 상태의 일수입니다. 기본값은 30입니다. 제약 없음
c18d2gz128 수명 주기 정책이 구성되지 않은 Amazon ECR 리포지토리	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy 수명 주기 정책이 아직 없는 경우 지정된 리포지토리에 대한 수명 주기 정책을 생성합니다.	ImageAgeLimit: Amazon ECR 리포지토리의 'any' 이미지에 대한 일(1~365) 단위의 최대 수명 제한입니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
DAvU99Dc4C 사용률이 낮은 Amazon EBS 볼륨	AWSManagedServices-DeleteUnusedEBSVolume 지난 7일 동안 볼륨이 연결되지 않은 경우 사용률이 낮은 Amazon EBS 볼륨을 삭제합니다. Amazon EBS 스냅샷은 기본적으로 생성됩니다.	• CreateSnapshot: 로 설정하면 true 자동화가 삭제되기 전에 Amazon EBS 볼륨의 스냅샷을 생성합니다. 기본 설정은 true입니다. 유효한 값은 true 및 false (대/소문자 구분)입니다. • MinimumUnattachedDays: 삭제할 EBS 볼륨의 연결되지 않은 최소 일수, 최대 62일. 로 설정하면 0 SSM 문서는 연결되지 않은 기간을 확인하지 않고 볼륨이 현재 연결되지 않은 경우 볼륨을 삭제합니다. 기본값은 7입니다. 제약 없음
hjLMh88uM8 유휴 로드 밸런서	AWSManagedServices-DeleteIdleClassicLoadBalancer 사용되지 않고 등록된 인스턴스가 없는 경우 유휴 Classic Load Balancer를 삭제합니다.	IdleLoadBalancerDays: Classic Load Balancer가 유휴 상태로 간주하기 전에 연결을 요청한 일수입니다. 기본값은 7일입니다. 자동 실행이 활성화된 경우 활성 백엔드 인스턴스가 없는 경우 자동화는 유휴 Classic Load Balancer를 삭제합니다. 활성 백엔드 인스턴스가 있지만 정상 백엔드 인스턴스가 없는 모든 유휴 Classic Load Balancer의 경우 자동 문제 해결이 사용되지 않으며 수동 문제 해결을 위한 OpsItems이 생성됩니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Ti39halfu8 Amazon RDS 유휴 DB 인스턴스	AWSManagedServices-StopIdleRDSInstance 지난 7일 동안 유휴 상태였던 Amazon RDS DB 인스턴스가 중지됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
COr6dfpM05 AWS Lambda 메모리 크기에 대한 과다 프로비저닝된 함수	AWSManagedServices-ResizeLambdaMemory AWS Lambda 함수의 메모리 크기가에서 제공하는 권장 메모리 크기로 조정됩니다 Trusted Advisor.	RecommendedMemorySize: Lambda 함수에 대한 권장 메모리 할당입니다. 값 범위는 128~10240입니다. 자동화가 실행되기 전에 Lambda 함수 크기가 수정된 경우이 자동화에서 권장 값으로 설정을 덮어쓸 수 있습니다 Trusted Advisor.
Qch7DwouX1 낮은 사용률의 Amazon EC2 인스턴스	AWSManagedServices-StopEC2Instance(자동 및 수동 실행 모드 모두에 대한 기본 SSM 문서) 사용률이 낮은 Amazon EC2 인스턴스는 중지됩니다.	ForceStopWithInstanceStore: 인스턴스 스토어를 사용하여 인스턴스를 강제 중지true하려면 로 설정합니다. 그렇지 않으면 false(으)로 설정합니다. 의 기본값은 인스턴스 중지를 false 방지합니다. 유효한 값은 true 또는 false(대/소문자 구분)입니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Qch7DwouX1 낮은 사용률의 Amazon EC2 인스턴스	AWSManagedServices-ResizeInstanceByOneLevel Amazon EC2 인스턴스는 동일한 인스턴스 패밀리 유형에서 하나의 인스턴스 유형으로 크기가 조정됩니다. 크기 조정 작업 중에 인스턴스가 중지 및 시작되고 SSM 문서 실행이 완료된 후 초기 상태로 돌아갑니다. 이 자동화는 Auto Scaling 그룹에 있는 인스턴스의 크기 조정을 지원하지 않습니다.	• MinimumDaysSinceLastChange: 마지막 인스턴스 유형 변경 이후 최소 일수입니다. 인스턴스 유형이 지정된 시간 내에 수정된 경우 인스턴스 유형은 변경되지 않습니다. 0를 사용하여이 검증을 건너뛰니다. 기본값은 7입니다. • CreateAMIBeforeResize: 크기를 조정하기 전에 인스턴스 AMI를 백업으로 생성하려면를 선택합니다true. 백업을 생성하지 않으려면를 선택합니다false. 기본값은 false입니다. 유효한 값은 true 및 false (대소문자 구분)입니다. • ResizeIfStopped: 인스턴스가 중지된 상태인 경우에도 인스턴스 크기 변경을 진행하려면를 선택합니다true. 중지된 상태인 경우 인스턴스의 크기를 자동으로 조정하지 않으려면를 선택합니다false. 유효한 값은 true 및 false (대/소문자 구분)입니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Qch7DwouX1 낮은 사용률의 Amazon EC2 인스턴스	AWSManagedServices-TerminateInstance Auto Scaling 그룹의 일부가 아니고 종료 방지 기능이 활성화되지 않은 경우 활용률이 낮은 Amazon EC2 인스턴스가 종료됩니다. AMI는 기본적으로 생성됩니다.	CreateAMIBeforeTermination: EC2 인스턴스를 종료하기 전에 인스턴스 AMI를 백업으로 생성false하려면 이 옵션을 true 또는 로 설정합니다. 기본값은 true입니다. 유효한 값은 true 및 false (대소문자 구분)입니다. 제약 없음
G31sQ1E9U Underutilized Amazon Redshift Clusters	AWSManagedServices-PauseRedshiftCluster Amazon Redshift 클러스터가 일시 중지되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
c1cj39rr6v Amazon S3 불완전 멀티파트 업로드 중단 구성	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload Amazon S3 버킷은 특정 일 후에도 불완전하게 유지되는 멀티파트 업로드를 중단하도록 수명 주기 규칙으로 구성됩니다.	DaysAfterInitiation: Amazon S3가 불완전한 멀티파트 업로드를 중지한 이후의 일수입니다. 기본값은 7일로 설정됩니다. 제약 없음
c1z7kmr00n 인스턴스에 대한 Amazon EC2 비용 최적화 권장 사항	의 Amazon EC2 인스턴스 권장 사항 및 유휴 Amazon EC2 인스턴스를 사용합니다 Trusted Remediator에서 지원하는 Compute Optimizer 권장 사항 .	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c1z7kmr02n 볼륨에 대한 Amazon EBS 비용 최적화 권장 사항	에서 Amazon EBS 볼륨 권장 사항 및 유휴 Amazon EBS 볼륨을 사용합니다 Trusted Remediator에서 지원하는 Compute Optimizer 권장 사항 .	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
c1z7kmr03n DB 인스턴스에 대한 Amazon RDS 비용 최적화 권장 사항	의 유휴 Amazon RDS 인스턴스를 사용합니다 Trusted Remediator에서 지원하는 Compute Optimizer 권장 사항 .	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
c1z7kmr05n AWS Lambda 함수에 대한 비용 최적화 권장 사항	의 Lambda 함수 권장 사항을 사용합니다 Trusted Remediator에서 지원하는 Compute Optimizer 권장 사항 .	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음

Trusted Advisor Trusted Remediator에서 지원하는 보안 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
12Fnkpl8Y5 노출된 액세스 키	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey 노출된 IAM 액세스 키가 비활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 노출된 IAM 액세스 키로 구성된 애플리케이션은 인증할 수 없습니다.
Hs4Ma3G127 - API Gateway REST 및 WebSocket API	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging	LogLevel: 실행 로깅을 활성화하는 로깅 수준 ERROR - 로깅은 오류에 대해서만 활성화됩니다. INFO - 모든 이벤트에 대해 로깅이 활성화됩니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
실행 로깅을 활성화해야 합니다. 해당 AWS Security Hub 검사: APIGateway.y.1	실행 로깅은 API 단계에서 활성화됩니다.	실행 로그를 활성화하려면 계정의 CloudWatch에 로그를 읽고 쓸 수 있는 API Gateway 권한을 부여해야 합니다. 자세한 내용은 API Gateway에서 REST APIs에 대한 CloudWatch 로깅 설정을 참조하세요.
Hs4Ma3G129 - API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: APIGateway.y.3	AWSManagedServices-EnableApiGatewayXRayTracing X-Ray 추적은 API 단계에서 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
Hs4Ma3G202 - API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다. 해당 AWS Security Hub 검사: APIGateway.y.5	AWSManagedServices-EnableAPIGatewayCacheEncryption API Gateway REST API 단계에 캐시가 활성화된 경우 API Gateway REST API 캐시 데이터에 대해 유틸리티를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G177 - 해당 AWS Security Hub 검사 - 로드 밸런서와 연결된 Auto Scaling 그룹은 로드 밸런서 상태 확인 AutoScaling.1	AWSManagedServices-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck Auto Scaling 그룹에 대해 Elastic Load Balancing 상태 확인이 활성화됩니다.	HealthCheckGracePeriod: Auto Scaling이 서비스되는 Amazon Elastic Compute Cloud 인스턴스의 상태를 확인하기 전에 대기하는 초 단위 시간입니다. Auto Scaling 그룹에 연결된 Elastic Load Balancing 로드 밸런서 중 하나라도 비정상으로 보고하면 Elastic Load Balancing 상태 확인을 켜면 실행 중인 인스턴스가 교체될 수 있습니다. 자세한 내용은 Auto Scaling 그룹에 Elastic Load Balancing 로드 밸런서 연결을 참조하세요.
Hs4Ma3G245 - AWS CloudFormation 스택은 Amazon Simple Notification Service와 통합되어야 합니다. 해당 AWS Security Hub 검사: CloudFormation.1	AWSManagedServices-EnableCFNStackNotification CloudFormation 스택을 Amazon SNS 주제와 연결하여 알림을 받습니다.	NotificationARNs 선택한 CloudFormation 스택과 연결할 Amazon SNS 주제의 ARNs입니다. 자동 문제 해결을 활성화하려면 NotificationARNs 사전 구성된 파라미터를 제공해야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G210 - CloudFront 배포에는 로깅이 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: CloudFront.2	AWSManagedServices-EnableCloudFrontDistributionLogging Amazon CloudFront 배포에 대해 로깅이 활성화됩니다.	• BucketName: 액세스 로그를 저장할 Amazon S3 버킷의 이름입니다. • S3KeyPrefix: theAmazonCloudFront 배포 로그의 S3 버킷에 있는 위치의 접두사입니다. • IncludeCookies: 액세스 로그에 쿠키를 포함할지 여부를 나타냅니다. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. • BucketName • S3KeyPrefix • IncludeCookies 이 문제 해결 제약 조건은 CloudFront 배포에 대한 로깅을 켜려면 어떻게 해야 하나요?를 참조하세요.
Hs4Ma3G109 - CloudTrail 로그 파일 검증을 활성화해야 합니다. 해당 AWS Security Hub 검사: CloudTrail.4	AWSManagedServices-TrustedRemediatorEnableCloudTrailLoggingValidation CloudTrail 추적 로그 검증을 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G108 - CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다. 해당 AWS Security Hub 검사: CloudTrail.5	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail 는 CloudWatch Logs 와 통합됩니다.	- CloudWatchLogsLogGroupName: CloudTrail 로그가 전달되는 CloudWatch Logs 로그 그룹의 이름입니다. 계정에 있는 로그 그룹을 사용해야 합니다. - CloudWatchLogsRoleName: 사용자의 로그 그룹에 쓰기 위해 말을 CloudWatch Logs 엔드포인트의 IAM 역할 이름입니다. 계정에 있는 역할을 사용해야 합니다. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. - CloudWatchLogsLogGroupName - CloudWatchLogsRoleName
Hs4Ma3G217 - CodeBuild 프로젝트 환경에 로깅 AWS 구성이 있어야 합니다. 해당 AWS Security Hub 검사: CodeBuild.4	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig CodeBuild 프로젝트에 대한 로깅을 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G306 - Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: DocumentD B.3	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot Amazon DocumentDB 수동 클러스터 스냅샷에서 퍼블릭 액세스를 제거합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G308 - Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: DocumentD B.5	AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection Amazon DocumentDB 클러스터에 대한 삭제 보호를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G323 - DynamoDB 테이블에 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: DynamoDB.6	AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection 비 AMS DynamoDB 테이블에 대한 삭제 보호를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
ePs02jT06w - Amazon EBS 퍼블릭 스냅샷	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot Amazon EBS 스냅샷에 대한 퍼블릭 액세스가 비활성화되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G118 - VPC 기본 보안 그룹은 인바운드 또는 아웃바운드 트래픽을 허용해서는 안 됩니다. 해당 AWS Security Hub 검사: EC2.2	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG 기본 보안 그룹의 모든 수신 및 송신 규칙이 제거됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G117 - 연결된 EBS 볼륨은 유틸리티 시 암호화되어야 합니다. 해당 AWS Security Hub 검사: EC2.3	AWSManagedServices-EncryptInstanceVolume 인스턴스에 연결된 Amazon EBS 볼륨이 암호화됩니다.	- 볼륨을 암호화하기 위한 KMSKeyId: AWS KMS key ID 또는 ARN입니다. - DeleteStaleNonEncryptedSnapshotBackups: 암호화되지 않은 이전 볼륨의 스냅샷 백업을 삭제할지 여부를 결정하는 플래그입니다. 가 복원에 false 도움이 되도록 로 설정된 경우 문제 해결 및 롤백의 일부로 인스턴스DeleteStaleNonEncryptedSnapshotBackups 가 재부팅될 수 있습니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G120 - 중지된 EC2 인스턴스는 지정된 기간 후에 제거해야 합니다. 해당 AWS Security Hub 검사: EC2.4	AWSManagedServices-TerminateInstance(자동 및 수동 실행 모드 모두에 대한 기본 SSM 문서) 30일 동안 중지된 Amazon EC2 인스턴스는 종료됩니다.	CreateAMIBeforeTermination: EC2 인스턴스를 종료하기 전에 인스턴스 AMI를 백업으로 생성하려면 선택합니다true. 종료하기 전에 백업을 생성하지 않으려면 선택합니다false. 기본값은 true입니다. 제약 조건 없음
Hs4Ma3G120 - 중지된 EC2 인스턴스는 지정된 기간 후에 제거해야 합니다. 해당 AWS Security Hub 검사: EC2.4	AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - Security Hub에 정의된 일수 동안 중지된 Amazon EC2 인스턴스(기본값은 30)가 종료됩니다.	CreateAMIBeforeTermination: EC2 인스턴스를 종료하기 전에 인스턴스 AMI를 백업으로 생성하려면 선택합니다true. 종료하기 전에 백업을 생성하지 않으려면 선택합니다false. 기본값은 true입니다. 제약 조건 없음
Hs4Ma3G121 - EBS 기본 암호화를 활성화해야 합니다. 해당 AWS Security Hub 검사: EC2.7	AWSManagedServices-EncryptEBSByDefault Amazon EBS 암호화는 기본적으로 특정에 대해 활성화됩니다. AWS 리전	사전 구성된 파라미터는 허용되지 않습니다. 암호화 기본 제공은 리전별 설정입니다. 리전에 대해 활성화하면 해당 리전의 개별 볼륨 또는 스냅샷에 대해 비활성화할 수 없습니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G124 - Amazon EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다. 해당 AWS Security Hub 검사: EC2.8	AWSManagedServices-TrustedRolemediatorEnableEC2InstanceIMDSv2 Amazon EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용합니다.	- IMDSv1MetricCheckPeriod: CloudWatch에서 IMDSv1 사용량 지표를 분석할 일수(42-455)입니다. Amazon EC2 인스턴스가 지정된 기간 내에 생성된 경우 분석은 인스턴스 생성일부터 시작됩니다. - HttpPutResponseHopLimit: 인스턴스 메타데이터 토큰에 허용되는 최대 네트워크 홉 수입니다. 이 값은 1와 2 홉 간에 구성할 수 있습니다. 홉 제한은 인스턴스에서 직접 실행되는 프로세스에 대한 토큰 액세스를 1 제한하는 반면, 홉 제한은 인스턴스에서 실행되는 컨테이너에서의 액세스를 2 허용합니다. 제약 조건 없음
Hs4Ma3G207 - EC2 서브넷이 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다. 해당 AWS Security Hub 검사: EC2.15	AWSManagedServices-UpdateAutoAssignPublicIpv4Addresses VPC 서브넷은 퍼블릭 IP 주소를 자동으로 할당하지 않도록 구성됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G209 - 미사용 네트워크 액세스 제어 목록이 제거됨 해당 AWS Security Hub 검사: EC2.16	AWSManagedServices-DeleteUnusedNACL 미사용 네트워크 ACL 삭제	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G215 - 미사용 Amazon EC2 보안 그룹은 제거해야 합니다. 해당 AWS Security Hub 검사: EC2.22	AWSManagedServices-DeleteSecurityGroups 사용하지 않는 보안 그룹을 삭제합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G247 - Amazon EC2 Transit Gateway가 VPC 연결 요청을 자동으로 수락해서는 안 됩니다. 해당 AWS Security Hub 검사: EC2.23	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach - 지정된 비 AMS Amazon EC2 Transit Gateway에 대한 VPC 연결 요청의 자동 수락을 비활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G235 - ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다. 해당 AWS Security Hub 검사: ECR.2	AWSManagedServices-TrustedR emediatorSetImageTagImmutability 지정된 리포지토리에 대한 이미지 태그 변경 가능성 설정을 IMMUTABLE로 설정합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G216 - ECR 리포지토리에는 하나 이상의 수명 주기 정책이 구성되어 있어야 합니다. 해당 AWS Security Hub 검사: ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy ECR 리포지토리에는 수명 주기 정책이 구성되어 있습니다.	LifecyclePolicyText: 리포지토리에 적용할 JSON 리포지토리 정책 텍스트입니다. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. LifecyclePolicyText
Hs4Ma3G325 - EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: EKS.8	AWSManagedServices-TrustedR emediatorEnableEKSAuditLog EKS 클러스터에 대해 감사 로그가 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G183 - HTTP 헤더를 삭제하도록 애플리케이션 로드 밸런서를 구성해야 합니다. 해당 AWS Security Hub 검사: ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer가 잘못된 헤더 필드로 구성되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
Hs4Ma3G184 - Application Load Balancer 및 Classic Load Balancer 로깅을 활성화해야 합니다. 해당 AWS Security Hub 검사: ELB.5	AWSManagedServices-EnableELBLogging(자동 및 수동 실행 모드 모두에 대한 기본 SSM 문서) Application Load Balancer 및 Classic Load Balancer 로깅이 활성화되어 있습니다.	• BucketName: 버킷 이름(ARN 아님). 버킷 정책이 로깅을 위해 올바르게 구성되어 있는지 확인합니다. • S3KeyPrefix: Elastic Load Balancing 로그에 대한 Amazon S3 버킷 위치의 접두사입니다. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. • BucketName • S3KeyPrefix Amazon S3 버킷에는 버킷에 액세스 로그를 쓸 수 있는 권한을 Elastic Load Balancing에 부여하는 버킷 정책이 있어야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G18 4 - Application Load Balancer 및 Classic Load Balancer 로깅을 활성화해야 합니다. 해당 AWS Security Hub 검사: ELB.5	AWSManagedServices-EnableELBLoggingV2 Application Load Balancer 및 Classic Load Balancer 로깅이 활성화되어 있습니다.	• TargetBucketTagKey: 대상 Amazon S3 버킷을 식별하는 데 사용되는 태그 이름(대소문자 구분)입니다. 와 함께 사용하여 액세스 로깅을 위한 대상 버킷 역할을 할 버킷에 TargetBucketTagValue 태그를 지정합니다. • TargetBucketTagValue: 대상 Amazon S3 버킷을 식별하는 데 사용되는 태그 값(대소문자 구분)입니다. 와 함께 사용하여 액세스 로깅을 위한 대상 버킷 역할을 할 버킷에 TargetBucketTagKey 태그를 지정합니다. • S3BucketPrefix: Amazon S3 버킷의 접두사(논리적 계층 구조)입니다. 지정하는 접두사에는 문자열 AWSLogs가 포함되지 않아야 합니다. 자세한 내용은 접두사를 사용한 객체 구성을 참조하세요. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix Amazon S3 버킷에는 버킷에 액세스 로그를 쓸 수 있는 권한을 Elastic Load Balancing에 부여하는 버킷 정책이 있어야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G326 - Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다. 해당 AWS Security Hub 검사: EMR.2	AWSManagedServices-TrustedR emediatorEnableEMRBlockPublicAccess 계정에 대해 Amazon EMR 퍼블릭 액세스 차단 설정이 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
Hs4Ma3G135 - AWS KMS 키를 실수로 삭제해서는 안 됩니다. 해당 AWS Security Hub 검사: KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS 키 삭제가 취소되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
Hs4Ma3G299 - Amazon DocumentDB 수동 클러스터 스냅샷은 퍼블릭이어서는 안 됩니다. 해당 AWS Security Hub 검사: Neptune.4	AWSManagedServices-TrustedR emediatorEnableNeptuneDBClusterDeletionProtection Amazon Neptune 클러스터에 대한 삭제 보호를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G319 - Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: NetworkFirewall.9	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection - AWS Network Firewall에 대한 삭제 보호를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
Hs4Ma3G223 - OpenSearch 도메인은 노드 간에 전송된 데이터를 암호화해야 합니다. 해당 AWS Security Hub 검사: OpenSearch.3	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption 도메인에 대해 노드 간 암호화가 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. node-to-node 암호화가 활성화된 후에는 설정을 비활성화할 수 없습니다. 대신 암호화된 도메인의 수동 스냅샷을 만들고, 다른 도메인을 생성하고, 데이터를 마이그레이션한 다음 이전 도메인을 삭제합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G222 - CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅을 활성화해야 합니다. 해당 AWS Security Hub 검사: Opensearch h.4	AWSManagedServices-EnableOpenSearchLogging OpenSearch 도메인에 대해 오류 로깅이 활성화되어 있습니다.	CloudWatchLogGroupArn: anAmazon CloudWatch Logs 로그 그룹의 ARN입니다. 자동 문제 해결을 활성화하려면 미리 구성된 파라미터인 CloudWatchLogGroupArn을 제공해야 합니다. Amazon CloudWatch 리소스 정책은 권한으로 구성해야 합니다. 자세한 내용은 Amazon OpenSearch Service 사용 설명서의 감사 로그 활성화를 참조하세요.
Hs4Ma3G221 - OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: Opensearch h.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch 도메인은 감사 로깅이 활성화된 상태로 구성됩니다.	CloudWatchLogGroupArn: 로그를 게시할 CloudWatch Logs 그룹의 ARN입니다. 자동 문제 해결을 활성화하려면 미리 구성된 파라미터를 제공해야 합니다. CloudWatchLogGroupArn Amazon CloudWatch 리소스 정책은 권한으로 구성해야 합니다. 자세한 내용은 Amazon OpenSearch Service 사용 설명서의 감사 로그 활성화를 참조하세요.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G220 - OpenSearch 도메인에 대한 연결은 TLS 1.2를 사용하여 암호화해야 합니다. 해당 AWS Security Hub 검사: Opensearch.h.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 TLS 정책은 `Policy-Min-TLS-1-2-2019-07`로 설정되며 HTTPS(TLS)를 통한 암호화된 연결만 허용됩니다.	사전 구성된 파라미터는 허용되지 않습니다. TLS 1.2를 사용하려면 OpenSearch 도메인에 연결해야 합니다. 전송 중 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 이 기능으로 애플리케이션을 테스트하여 성능 프로파일과 TLS의 영향을 이해합니다.
Hs4Ma3G194 - Amazon RDS 스냅샷은 프라이빗이어야 합니다. 해당 AWS Security Hub 검사: RDS.1	AWSManagedServices-DisablePublicAccessOnRDSnapshotV2 Amazon RDS 스냅샷에 대한 퍼블릭 액세스가 비활성화되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
Hs4Ma3G192 - RDS DB 인스턴스는 PubliclyAccessible AWS 구성에 따라 퍼블릭 액세스를 금지해야 합니다. 해당 AWS Security Hub 검사: RDS.2	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance RDS DB 인스턴스에서 퍼블릭 액세스를 비활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G189 - Amazon RDS DB 인스턴스에 대해 향상된 모니터링이 구성됨 해당 AWS Security Hub 검사: RDS.6	AWSManagedServices-TrustedR emediatorEnableRDSEnhancedM onitoring Amazon RDS DB 인스턴스에 대한 향상된 모니터링 활성화	- MonitoringInterval: DB 인스턴스에 대해 Enhanced Monitoring 지표가 수집되는 시점 사이의 초 단위 간격입니다. 유효한 간격은 0, 1, 5, 10, 15, 30, 60입니다. 확장 모니터링 지표의 수집을 비활성화하려면 0을 지정합니다. - MonitoringRoleName: Amazon RDS가 향상된 모니터링 지표를 Amazon CloudWatch Logs로 전송하도록 허용하는 IAM 역할의 이름입니다. 역할을 지정하지 않으면 기본 역할rds-monitoring-role 이 사용되거나 존재하지 않는 경우 기본 역할이 생성됩니다. 자동화 실행 전에 향상된 모니터링이 활성화된 경우이 자동화는 사전 구성된 파라미터에 구성된 MonitoringInterval 및 MonitoringRoleName 값을 사용하여 설정을 덮어쓸 수 있습니다.
Hs4Ma3G190 - Amazon RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: RDS.7	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection Amazon RDS 클러스터에 대해 삭제 방지가 활성화되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G198 - Amazon RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: RDS.8	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection Amazon RDS 인스턴스에 대해 삭제 방지가 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G199 - RDS DB 인스턴스는 CloudWatch Logs에 로그를 게시해야 합니다. 해당 AWS Security Hub 검사: RDS.9	AWSManagedServices-TrustedR emediatorEnableRDSLogExports RDS DB 인스턴스 또는 RDS DB 클러스터에 대해 RDS 로그 내보내기가 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 서비스 연결 역할 AWSServiceRoleForRDS가 필요합니다.
Hs4Ma3G160 - RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다. 해당 AWS Security Hub 검사: RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management RDS 인스턴스에 대해 인증이 활성화됩니다.	ApplyImmediately:이 요청의 수정 사항과 보류 중인 수정 사항이 최대한 빨리 비동기적으로 적용되는지 여부를 나타냅니다. 변경 사항을 즉시 적용하려면 <code>true</code>를 선택합니다. 다음 유지 관리 기간에 대한 변경을 예약하려면 <code>false</code>를 선택합니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G161 - RDS 클러스터에 대해 IAM 인증을 구성해야 합니다. 해당 AWS Security Hub 검사: RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication RDS 클러스터에 대해 IAM 인증이 활성화됩니다.	ApplyImmediately: 이 요청의 수정 사항과 보류 중인 수정 사항이 최대한 빨리 비동기식으로 적용되는지 여부를 나타냅니다. 변경 사항을 즉시 적용하려면 <code>true</code>를 선택합니다. 다음 유지 관리 기간에 대한 변경을 예약하려면 <code>false</code>를 선택합니다. 제약 조건 없음
Hs4Ma3G162 - RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다. 해당 AWS Security Hub 검사: RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade Amazon RDS에 대한 마이너 버전 자동 업그레이드 구성이 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 문제 해결을 수행하려면 Amazon RDS 인스턴스가 <code>available</code> 상태여야 합니다.
Hs4Ma3G163 - 스냅샷에 태그를 복사하도록 RDS DB 클러스터를 구성해야 합니다. 해당 AWS Security Hub 검사: RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagToSnapshot Amazon RDS 클러스터에 대한 설정이 활성화되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 문제 해결을 수행하려면 Amazon RDS 인스턴스가 사용 가능한 상태여야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G164 - 스냅샷에 태그를 복사하도록 RDS DB 인스턴스를 구성해야 합니다. 해당 AWS Security Hub 검사: RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagsToSnapshot Amazon RDS에 대한 설정이 활성화되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 문제 해결을 수행하려면 Amazon RDS 인스턴스가 사용 가능한 상태여야 합니다.
rSs93HQwa1 Amazon RDS 퍼블릭 스냅샷	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Amazon RDS 스냅샷에 대한 퍼블릭 액세스가 비활성화되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G103 - Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다. 해당 AWS Security Hub 검사: Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster Amazon Redshift 클러스터의 퍼블릭 액세스가 비활성화되었습니다.	사전 구성된 파라미터는 허용되지 않습니다. 퍼블릭 액세스를 비활성화하면 인터넷에서 들어오는 모든 클라이언트가 차단됩니다. 그리고 Amazon Redshift 클러스터는 몇 분 동안 수정 상태인 반면 수정은 클러스터에 대한 퍼블릭 액세스를 비활성화합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G106 - Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: Redshift.4	AWSManagedServices-TrustedRedshiftClusterAuditLogging 유지 관리 기간 동안 Amazon Redshift 클러스터에 대한 감사 로깅이 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 자동 문제 해결을 활성화하려면 다음과 같은 사전 구성된 파라미터를 제공해야 합니다. BucketName: 버킷이 동일해야 합니다 AWS 리전. 클러스터에는 읽기 버킷이 있어야 하며 객체 권한을 부여해야 합니다. 자동화 실행 전에 Redshift 클러스터 로깅이 활성화된 경우이 자동화에 사전 구성된 파라미터에 구성된 BucketName 및 S3KeyPrefix 값으로 로깅 설정을 덮어쓸 수 있습니다.
Hs4Ma3G105 - Amazon Redshift는 메이저 버전으로 자동 업그레이드가 활성화되어 있어야 합니다. 해당 AWS Security Hub 검사: Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade - 메이저 버전 업그레이드는 유지 관리 기간 동안 클러스터에 자동으로 적용됩니다. Amazon Redshift 클러스터에는 즉각적인 가동 중지가 없지만 메이저 버전으로 업그레이드하는 경우 유지 관리 기간 동안 Amazon Redshift 클러스터에 가동 중지가 발생할 수 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G104 - Amazon Redshift 클러스터는 항상 된 VPC 라우팅을 사용해야 합니다. 해당 AWS Security Hub 검사: Redshift.7	AWSManagedServices-TrustedRedshiftClusterEnhancedVPCRouting Amazon Redshift 클러스터에 대해 항상 된 VPC 라우팅이 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
Hs4Ma3G173 - 버킷 수준에서 S3 퍼블릭 액세스 차단 설정을 활성화해야 합니다. 해당 AWS Security Hub 검사: S3.8	AWSManagedServices-TrustedRedshiftClusterEnhancedVPCRouting 버킷 수준 퍼블릭 액세스 블록은 Amazon S3 버킷에 적용됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 수정 사항은 S3 객체 가용성에 영향을 미칠 수 있습니다. Amazon S3가 액세스를 평가하는 방법에 대한 자세한 내용은 Amazon S3 스토리지에 대한 퍼블릭 액세스 차단을 참조하세요.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G230 - S3 버킷 서버 액세스 로깅을 활성화해야 합니다. 해당 AWS Security Hub 검사: S3.9	AWSManagedServices-EnableBucketAccessLogging(자동 및 수동 실행 모드 모두에 대한 기본 SSM 문서) Amazon S3 서버 액세스 로깅이 활성화되었습니다.	• TargetBucket: 서버 액세스 로그를 저장할 S3 버킷의 이름입니다. • TargetObjectKeyFormat: 로그 객체의 Amazon S3 키 형식(값은 대/소문자를 구분함). 로그 객체에 대한 S3 키의 단순 형식을 사용하려면 SimplePrefix . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 EventTime을 사용하려면 PartitionedPrefixEventTime . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 DeliveryTime을 사용하려면 PartitionedPrefixDeliveryTime . 유효 값은 SimplePrefix , PartitionedPrefixEventTime 및 PartitionedPrefixDeliveryTime 입니다. 자동 문제 해결을 활성화하려면 사전 구성된 파라미터인 TargetBucket을 제공해야 합니다. 대상 버킷은 로그 전송에 대한 올바른 권한을 가진 원본 버킷과 동일한 AWS 리전 및 AWS 계정 에 있어야 합니다. 자세한 내용은 Amazon S3 서버 액세스 로깅 활성화를 참조하세요.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G230 – S3 버킷 서버 액세스 로깅을 활성화해야 합니다. 해당 AWS Security Hub 검사: S3.9	AWSManagedServices-TrustedR emediatorEnableBucketAccess LoggingV2 - Amazon S3 버킷 로깅이 활성화되어 있습니다.	• TargetBucketTagKey: 대상 버킷을 식별하기 위한 태그 이름(대소문자 구분)입니다. 이 및 TargetBucketTagValue를 사용하여 액세스 로깅의 대상 버킷으로 사용할 버킷에 태그를 지정합니다. • TargetBucketTagValue: 대상 버킷을 식별하기 위한 태그 값(대소문자 구분)으로, 이 및 TargetBucketTagKey를 사용하여 액세스 로깅을 위한 대상 버킷으로 사용할 버킷에 태그를 지정합니다. • TargetObjectKeyFormat: 로그 객체의 Amazon S3 키 형식(값은 대소문자를 구분함): 로그 객체의 S3 키에 단순 형식을 사용하려면 SimplePrefix를 선택합니다. 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 EventTime을 사용하려면 PartitionedPrefixEventTime을 선택합니다. 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 DeliveryTime을 사용하려면 PartitionedPrefixDeliveryTime을 선택합니다. 기본값은 PartitionedPrefixEventTime입니다. 자동 문제 해결을 활성화하려면 TargetBucketTagKey 및 TargetBucketTagValue 파라미터를 제공해야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		대상 버킷은 로그 전송에 대한 올바른 권한을 가진 원본 버킷과 동일한 AWS 리전 및 AWS 계정에 있어야 합니다. 자세한 내용은 Amazon S3 서버 액세스 로깅 활성화 를 참조하세요.
Pfx0RwqBli Amazon S3 버킷 권한	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess 퍼블릭 액세스 차단	사전 구성된 파라미터는 허용되지 않습니다. 이 검사는 여러 알림 기준으로 구성됩니다. 이 자동화는 퍼블릭 액세스 문제를 해결합니다. 에서 플래그가 지정된 Trusted Advisor 다른 구성 문제에 대한 수정은 지원되지 않습니다. 이 문제 해결은 AWS 서비스 생성된 S3 버킷 (예: cf-templates-000000000000) 문제 해결을 지원합니다.
Hs4Ma3G27 2 - 사용자에게 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다. 해당 AWS Security Hub 검사: SageMaker.3	AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess SageMaker 노트북 인스턴스에서는 사용자의 루트 액세스가 비활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 문제를 해결하면 SageMaker 노트북 인스턴스가 InService 상태인 경우 중단이 발생합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G179 - SNS 주제를를 사용하여 유희 시 암호화되어야 합니다. AWS KMS 해당 AWS Security Hub 검사: SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest SNS 주제는 서버 측 암호화로 구성됩니다.	KmsKeyId: 서버 측 암호화(SSE)에 사용할 Amazon SNS용 AWS 관리형 고객 마스터 키(CMK) 또는 사용자 지정 CMK의 ID입니다. 기본값은 로 설정됩니다alias/aws/sns . 사용자 지정 AWS KMS 키를 사용하는 경우 올바른 권한으로 구성해야 합니다. 자세한 내용은 Amazon SNS 주제에 대한 서버 측 암호화(SSE) 활성화를 참조하세요.
Hs4Ma3G158 - SSM 문서는 공개되어서는 안 됩니다. 해당 AWS Security Hub 검사: SSM.4	AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing - SSM 문서의 퍼블릭 공유를 비활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Hs4Ma3G136 - Amazon SQS 대기열은 저장 시 암호화되어야 합니다. 해당 AWS Security Hub 검사: SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest Amazon SQS의 메시지는 암호화됩니다.	• SqsManagedSseEnabled: Amazon SQS 소유 암호화 키를 사용하여 서버 측 대기열 암호화를 활성화하려면 <code>true</code>로 설정하고 키를 사용하여 서버 측 대기열 암호화를 활성화하려면 <code>false</code>로 설정합니다 AWS KMS . • KMSKeyId: 대기열의 서버 측 암호화에 사용할 Amazon SQS용 AWS 관리형 고객 마스터 키(CMK) 또는 사용자 지정 CMK의 ID 또는 별칭입니다. Amazon SQS 제공되지 않으면 <code>alias/aws/sqs</code> 사용됩니다. • KmsDataKeyReusePeriodSeconds: AWS KMS 다시 호출하기 전에 Amazon SQS가 데이터 키를 재사용하여 메시지를 암호화하거나 해독할 수 있는 초 단위의 시간 길이입니다. 초 단위의 정수로, 60초(1분)에서 86,400초(24시간) 사이입니다. 이 로 SqsManagedSseEnabled 설정된 경우이 설정은 무시됩니다 <code>true</code>. 암호화된 대기열에 대한 익명 SendMessage 및 ReceiveMessage 요청은 거부됩니다. SSE를 사용할 수 있는 대기열에 대한 모든 요청에서는 HTTPS 및 서명 버전 4를 사용해야 합니다.

Trusted Advisor Trusted Remediator에서 지원하는 내결함성 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c18d2gz138 Amazon DynamoDB의 지 점 실시간 복구	AWSManagedServices-TrustedRemediatorEnableDDBPITR DynamoDB 테이블에 대한 point-in-time으로 복구를 활성화합니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
R365s2Qddf Amazon S3 Bucket Versioning	AWSManagedServices-TrustedRemediatorEnableBucketVersioning Amazon S3 버킷 버전 관리가 활성화되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 문제 해결은 AWS 서비스 생성된 S3 버킷(예: cf-templates-0000000000000000)의 문제 해결을 지원하지 않습니다.
BueAdJ7NrP Amazon S3 버킷 로깅	AWSManagedServices-EnableBucketAccessLogging Amazon S3 버킷 로깅이 활성화되었습니다.	- TargetBucket: 서버 액세스 로그를 저장할 S3 버킷의 이름입니다. - TargetObjectKeyFormat: 로그 객체에 대한 Amazon S3 키의 간단한 형식을 사용하려면 로그 객체에 대한 Amazon S3 키 형식을 선택합니다 SimplePrefix . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 EventTime을 사용하려면를 선택합니다PartitionedPrefixEventTime . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 DeliveryTime을 사용하려면를 선택합니다PartitionedPrefixDeliveryTime . 기본값은 PartitionedPrefixEventTime 입니다. 유효한 값은 SimplePre

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		<code>fix</code> , <code>PartitionedPrefixEventTime</code> 및 <code>PartitionedPrefixDeliveryTime</code> (대소문자 구분)입니다. 자동 문제 해결을 활성화하려면 다음과 같이 미리 구성된 파라미터를 제공해야 합니다. • <code>TargetBucket</code> 대상 버킷은 로그 전송에 대한 올바른 권한을 가진 원본 버킷과 동일한 AWS 리전 및 AWS 계정에 있어야 합니다. 자세한 내용은 Amazon S3 서버 액세스 로깅 활성화를 참조하세요.
f2iK5R6Dep Amazon RDS 다중 AZ	<code>AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ</code> 다중 가용 영역 배포가 활성화되어 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 이 변경 중에 성능 저하가 발생할 수 있습니다.
H7lgTzjTYb Amazon EBS 스냅샷	<code>AWSManagedServices-TrustedRemediatorCreateEBSSnapshot</code> Amazon EBSsnapshots이 생성됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
opQPADkZvH RDS 백업	AWSManagedServices-EnableRDSBackupRetention DB에 대해 Amazon RDS 백업 보존이 활성화됩니다.	- BackupRetentionPeriod: 자동 백업을 보존할 일수(1~35일)입니다. - ApplyImmediately: RDS 백업 보존 변경 및 보류 중인 수정 사항이 가능한 한 빨리 비동기적으로 적용되는지 여부를 나타냅니다. 변경 사항을 즉시 true 적용하거나 다음 유지 관리 기간에 대한 변경 사항을 예약false하도록 선택합니다. ApplyImmediately 파라미터가 설정된 경우 truedb에서 보류 중인 변경 사항이 RDSBackup 보존 설정과 함께 적용됩니다.
c1qf5bt013 Amazon RDS DB 인스턴스의 스토리지 자동 크기 조정이 꺼져 있음	AWSManagedServices-TrustedR emediatorEnableRDSInstanceStorageAutoScaling - Amazon RDS DB 인스턴스에 대해 스토리지 자동 크기 조정이 활성화되어 있습니다.	MaxAllocatedStorageIncreasePercentage: AllocatedStorage를 설정하기 위한 현재 AllocatedStorage의 증가 비율입니다. MaxAllocatedStorage 기본값은 로 설정됩니다26. 최대 스토리지 임계값을 현재 할당된 스토리지보다 10% 이상 높게 설정해야 합니다. 최대 스토리지 임계값을 26% 이상으로 설정하는 것이 가장 좋습니다. 자세한 내용은 Amazon Relational Database Service 스토리지 자동 크기 조정을 사용하여 용량 자동 관리를 참조하세요. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
7qGXsKIUw Classic Load Balancer 연결 드레이닝	AWSManagedServices-TrustedR emediatorEnableCLBConnectio nDraining Classic Load Balancer에 대해 연결 드레이닝이 활성화되어 있습니다.	ConnectionDrainingTimeout: 인스턴스 등록을 취소하기 전에 기존 연결을 열어 두는 최대 시간입니다. 기본값은 300 초로 설정됩니다. 제약 조건 없음
c18d2gz106 Amazon EBS가 AWS Backup 플랜에 포함되지 않음	AWSManagedServices-TrustedR emediatorAddVolumeToBackupPlan Amazon EBS는 AWS Backup 플랜에 포함되어 있습니다.	문제 해결은 다음 태그 페어를 사용하여 Amazon EBS 볼륨에 태그를 지정합니다. 태그 페어는 태그 기반 리소스 선택 기준과 일치해야 합니다 AWS Backup. • TagKey • TagValue 제약 조건 없음
c18d2gz107 AWS Backup 계획에 포함되지 않은 Amazon DynamoDB 테이블	AWSManagedServices-TrustedR emediatorAddDynamoDBToBacku pPlanAddDynamoDBToBackupPlan Amazon DynamoDB 테이블은 AWS Backup 플랜에 포함되어 있습니다.	문제 해결은 다음 태그 페어를 사용하여 Amazon DynamoDB에 태그를 지정합니다. 태그 페어는 태그 기반 리소스 선택 기준과 일치해야 합니다 AWS Backup. • TagKey • TagValue 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c18d2gz117 Amazon EFS가 AWS Backup 플랜에 포함되지 않음	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS는 AWS Backup 플랜에 포함되어 있습니다.	문제 해결은 다음 태그 페어를 사용하여 Amazon EFS에 태그를 지정합니다. 태그 페어는 태그 기반 리소스 선택 기준과 일치해야 합니다 AWS Backup. • TagKey • TagValue 제약 조건 없음
c18d2gz105 Network Load Balancer 교차 로드 밸런싱	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing Network Load Balancer에서 교차 영역 로드 밸런싱이 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt026 Amazon RDS synchronous_commit 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS에 대해 파라미터synchronous_commit 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt030 Amazon RDS innodb_flush_log_at_trx_commit 파라미터가 아님 1	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS의 경우 파라미터innodb_flush_log_at_trx_commit 가 로 설정되어 1 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c1qf5bt031 Amazon RDS sync_binlog 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS에 대해 파라미터sync_binlog 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt036 Amazon RDS innodb_default_row_format 파라미터 설정이 안전하지 않음	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS의 경우 파라미터innodb_default_row_format 가 로 설정되어 DYNAMIC 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c18d2gz144 Amazon EC2 세부 모니터링이 활성화되지 않음	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring Amazon EC2에 대해 세부 모니터링이 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

Trusted Advisor Trusted Remediator에서 지원하는 성능 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
COr6dfpM06 AWS Lambda 메모리 크기에 대한 과소 프로비저닝된 함수	AWSManagedServices-ResizeLambdaMemory Lambda 함수 메모리 크기에서 제공하는 권장 메모리 크기로 조정됩니다 Trusted Advisor.	RecommendedMemorySize: Lambda 함수에 대한 권장 메모리 할당입니다. 값 범위는 128~10240입니다. 자동화 실행 전에 Lambda 함수 크기가 수정된 경우이 자동화에서 권장

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		하는 값으로 설정을 덮어쓸 수 있습니다 Trusted Advisor.
ZRxQIPsb6c 높은 사용률의 Amazon EC2 인스턴스	AWSManagedServices-ResizeInstanceByOneLevel Amazon EC2 인스턴스는 동일한 인스턴스 패밀리 유형에서 하나의 인스턴스 유형으로 크기가 조정됩니다. 인스턴스는 크기 조정 작업 중에 중지 및 시작되고 실행이 완료된 후 초기 상태로 돌아갑니다. 이 자동화는 Auto Scaling 그룹에 있는 인스턴스의 크기 조정을 지원하지 않습니다.	• MinimumDaysSinceLastChange: 마지막 인스턴스 유형이 변경된 이후 최소 일수입니다. 인스턴스 유형이 지정된 시간 내에 수정된 경우 인스턴스 유형은 변경되지 않습니다. 0를 사용하여이 검증을 건너뜁니다. 기본값은 7입니다. • CreateAMIBeforeResize: 크기를 조정하기 전에 인스턴스 AMI를 백업으로 생성하려면를 선택합니다true. 백업을 생성하지 않으려면를 선택합니다false. 기본값은 false입니다. 유효한 값은 true 및 false (대/소문자 구분)입니다. • ResizelfStopped: 인스턴스가 중지된 상태인 경우에도 인스턴스 크기 변경을 진행하려면를 선택합니다true. 중지된 상태인 경우 인스턴스의 크기를 자동으로 조정하지 않으려면를 선택합니다false. 유효한 값은 true 및 false (대소문자 구분)입니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c1qf5bt021 최적 값보다 작은 값을 사용하는 Amazon RDS innodb_change_buffering 파라미터	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS의 NONE 경우 innodb_change_buffering 파라미터 값이 로 설정됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt025 Amazon RDS autovacuum 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS에 대해 파라미터 autovacuum 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt028 Amazon RDS enable_indexonlyscan 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS에 대해 파라미터 enable_indexonlyscan 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt029 Amazon RDS enable_indexscan 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS에 대해 파라미터 enable_indexscan 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c1qf5bt032 Amazon RDS innodb_stats_persistent 파라미터가 꺼져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS에 대해 파라미터innodb_stats_persistent 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음
c1qf5bt037 Amazon RDS general_logging 파라미터가 켜져 있음	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS에 대해 파라미터general_logging 가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 조건 없음

Trusted Advisor Trusted Remediator에서 지원하는 서비스 제한 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
IN7RR0I7J9 EC2-VPC 탄력적 IP 주소	AWSManagedServices-UpdateVpcElasticIPQuota EC2-VPC 탄력적 IP 주소에 대한 새로운 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.
kM7QQ0I7J9 VPC 인터넷 게이트웨이	AWSManagedServices-IncreaseServiceQuota - VPC 인터넷 게이트웨이에 대한 새로운 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
jL7PP0i7J9 VPC	AWSManagedServices-Increase ServiceQuota VPC에 대한 새 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	실행되는 경우 더 높은 제한 증가가 있을 수 있습니다. 중분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.
fW7HH0i7J9 Auto Scaling 그룹	AWSManagedServices-Increase ServiceQuota Auto Scaling 그룹에 대한 새 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증가: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.
3Njm0DJQO9 RDS 옵션 그룹	AWSManagedServices-Increase ServiceQuota Amazon RDS 옵션 그룹에 대한 새로운 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	중분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.
EM8b3yLRTr ELB Application Load Balancers	AWSManagedServices-Increase ServiceQuota ELB Application Load Balancer에 대한 새로운 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증가: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
8wlqYSt25K ELB 네트워크 로드 밸런서	AWSManagedServices-IncreaseServiceQuota ELB Network Load Balancer에 대한 새로운 제한이 요청됩니다. 기본적으로 제한은 3씩 증가합니다.	증분: 현재 할당량을 늘릴 수 있습니다. 기본값은 3입니다. Trusted Advisor 점검이 OK 상태로 업데이트되기 전에이 자동화가 여러 번 실행되는 경우 더 높은 제한 증가가 있을 수 있습니다.

Trusted Advisor Trusted Remediator에서 지원하는 운영 우수성 검사

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c18d2gz125 Amazon API Gateway에서 실행 로그를 기록하지 않음	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging 실행 로깅은 API 단계에서 활성화됩니다.	사전 구성된 파라미터는 허용되지 않습니다. 실행 로그를 활성화하려면 API Gateway에 계정의 CloudWatch에 로그를 읽고 쓸 수 있는 권한을 부여해야 합니다. 자세한 내용은 API Gateway에서 REST APIs에 대한 CloudWatch 로깅 설정을 참조하세요 .
c18d2gz168 로드 밸런서에 Elastic Load Balancing 삭제 보호 기능이 활성화되지 않음	AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection - Elastic Load Balancer에 대해 삭제 방지가 켜져 있습니다.	사전 구성된 파라미터는 허용되지 않습니다. 제약 없음
c1qf5bt012	AWSManagedServices-TrustedRemediatorEnableRDSPerformanceInsights	PerformanceInsightsRetentionPeriod: 성능 개선 도우미 데이터를 보존할 일수입니다. 유효한 값: 7

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
Amazon RDS 성능 개선 도우미가 꺼져 있음	Amazon RDS에 대해 성능 개선 도우미가 켜져 있습니다.	또는 월 * 31. 여기서 월은 1~23개월의 개월 수입니다. 예: 93 (3개월 * 31), 341 (11개월 * 31), 589 (19개월 * 31) 또는 731. • PerformanceInsightsKMSKeyId: 성능 개선 도우미 데이터의 암호화를 위한 AWS KMS 키 ID입니다. PerformanceInsightsKMSKeyId 값을 지정하지 않으면 Amazon RDS가 기본 AWS KMS 키를 사용합니다. 제약 없음

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
c1fd6b9614 Amazon S3 액세스 로그 활성화됨	AWSManagedServices-TrustedRolemediatorEnableBucketAccessLoggingV2 Amazon S3 버킷 액세스 로깅이 활성화되었습니다.	• TargetBucketTagValue: 태그 값 (대소문자 구분)을 사용하여 대상 버킷을 식별하고,이 및 TargetBucketTagKey를 사용하여 액세스 로깅의 대상 버킷으로 사용할 버킷에 태그를 지정합니다. • TargetObjectKeyFormat: 로그 객체의 Amazon S3 키 형식(값은 대/소문자를 구분함). 로그 객체에 대한 S3 키의 단순 형식을 사용하려면 SimplePrefix . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 EventTime을 사용하려면 PartitionedPrefixEventTime . 로그 객체에 파티션된 S3 키를 사용하고 파티션된 접두사에 DeliveryTime을 사용하려면 PartitionedPrefixDeliveryTime . 유효 값은 SimplePrefix , PartitionedPrefixEventTime 및 PartitionedPrefixDeliveryTime 입니다. 자동 문제 해결을 활성화하려면 사전 구성된 파라미터인 TargetBucketTagKey 및 TargetBucketTagValue를 제공해야 합니다. 대상 버킷은 로그 전송에 대한 올바른 권한을 가진 원본 버킷과 동일한 AWS 리전 및 AWS 계정에 있어야 합니다.

ID 및 이름 확인	SSM 문서 이름 및 예상 결과	지원되는 사전 구성된 파라미터 및 제약 조건
		자세한 내용은 Amazon S3 서버 액세스 로그 활성화 를 참조하세요.

신뢰할 수 있는 수정자에서 Trusted Advisor 검사 수정 구성

구성은 Trusted Remediator 애플리케이션의 AWS AppConfig 일부로 저장됩니다. 각 Trusted Advisor 검사 범주에는 별도의 구성 프로필이 있습니다. Trusted Advisor 범주에 대한 자세한 내용은 [검사 범주 보기](#)를 참조하세요.

리소스별 또는 Trusted Advisor 검사별로 문제 해결을 구성하도록 요청할 수 있습니다. 리소스 태그를 사용하여 예외를 적용할 수 있습니다.

Note

조사 Trusted Advisor 결과 수정은 현재를 사용하여 구성되며 AWS AppConfig, 이 기능은 현재 완전히 지원됩니다. AMS는 향후 변경될 것으로 예상합니다. 이 방법은 변경될 수 AWS AppConfig 있으므로 의존하는 자동화를 빌드하지 않는 것이 가장 좋습니다. 호환성을 위해 향후 현재 AWS AppConfig 구현을 기반으로 구축된 자동화를 업데이트하거나 수정해야 할 수 있습니다.

Compute Optimizer -> EC2 인스턴스 기능 플러그에는 추가 파라미터가 있습니다.

- allow-upscale 과소 프로비저닝된 최적화되지 않은 EC2 인스턴스를 확장할 수 있습니다. 기본값은 "false"입니다.
- min-savings-opportunity-percentage 자동 문제 해결을 위한 최소 절감률 기회입니다. 기본값은 10%입니다.

기본 문제 해결 구성

개별 Trusted Advisor 검사에 대한 구성은 AWS AppConfig 플러그로 저장됩니다. 플러그 이름은 검사 이름과 일치합니다. 각 검사 구성에는 다음 속성이 포함됩니다.

- execution-mode: 신뢰할 수 있는 수정자가 기본 수정을 수행하는 방법을 결정합니다.
 - 자동: 신뢰할 수 있는 수정자는 OpsItem을 생성하고 SSM 문서를 실행한 다음 실행 성공 후 OpsItem을 해결하여 리소스를 자동으로 수정합니다.

- 수동: OpsItem이 생성되지만 SSM 문서가 자동으로 실행되지 않습니다. OpsItem을 검토하고 자동 RFC를 사용하여 문제 해결을 실행합니다. 자세한 내용은 [신뢰할 수 있는 수정자에서 문제 해결 작업](#) 단원을 참조하십시오.
- 조건부: 수정은 기본적으로 비활성화되어 있습니다. 태그를 사용하여 특정 리소스에 대해 활성화할 수 있습니다. 자세한 내용은 다음 섹션 [리소스 태그를 사용하여 문제 해결 사용자 지정](#) 및 단원을 참조하십시오. [리소스 재정의 태그를 사용하여 문제 해결 사용자 지정](#).
- 비활성: 수정이 발생하지 않고 OpsItem이 생성되지 않습니다. 비활성으로 설정된 Trusted Advisor 검사의 실행 모드는 재정의할 수 없습니다.
- pre configured-parameters: 자동 문제 해결에 필요한 SSM 문서 파라미터 값을 쉼표(,)로 Parameter=Value 구분하여 형식으로 입력합니다. 각 검사에 대해 연결된 SSM 문서에 대해 [Trusted Advisor Trusted Remediator에서 지원하는 검사](#) 지원되는 사전 구성된 파라미터는 섹션을 참조하세요.
- alternative-automation-document: 이 속성은 지원되는 다른 문서(특정 검사에 사용할 수 있는 경우)로 기존 자동화 문서를 재정의하는 데 도움이 됩니다. 기본적으로 이 속성은 선택되지 않습니다.

Note

alternative-automation-document 속성은 사용자 지정 자동화 문서를 지원하지 않습니다. 예 나열된 기존의 지원되는 Trusted Remediator 자동화 문서를 사용할 수 있습니다. [Trusted Advisor Trusted Remediator에서 지원하는 검사](#).

예를 들어, 검사에는 AWSManagedServices-StopEC2InstanceQch7DwouX1, AWSManagedServices-ResizeInstanceByOneLevel 및 AWSManagedServices-TerminateInstance의 세 가지 관련 SSM 문서가 있습니다. AWSManagedServices-StopEC2Instance의 값은 AWSManagedServices-ResizeInstanceByOneLevel 또는 AWSManagedServices-TerminateInstance일 alternative-automation-document 수 있습니다(AWSManagedServices-StopEC2Instance는를 해결하기 위한 기본 SSM 문서 임Qch7DwouX1).

각 속성의 값은 해당 속성의 제약 조건과 일치해야 합니다.

i Tip

Trusted Advisor 검사에 기본 구성을 적용하기 전에 다음 섹션에 설명된 리소스 태그 지정 및 리소스 재정의 기능을 사용하는 것이 좋습니다. 기본 구성은 계정 내 모든 리소스에 적용되며, 모든 경우에 바람직하지 않을 수 있습니다.

다음은 실행 모드가 수동으로 설정되고 속성이 제약 조건과 일치하는 예제 콘솔 스크린샷입니다.

리소스 태그를 사용하여 문제 해결 사용자 지정

검사 구성의 `automated-for-tagged-only` 및 `manual-for-tagged-only` 속성을 사용하면 개별 검사를 수정하는 방법에 대한 리소스 태그를 지정할 수 있습니다. 동일한 태그 또는 태그를 공유하는 리소스 그룹에 일관된 문제 해결 동작을 적용해야 하는 경우 이 방법을 사용하는 것이 가장 좋습니다. 다음은 이러한 태그에 대한 설명입니다.

- `automated-for-tagged-only`: 기본 실행 모드에 관계없이 자동으로 수정할 검사의 리소스 태그(하나 이상의 태그 페어, 쉼표로 구분)를 지정합니다.
- `manual-for-tagged-only`: 기본 실행 모드에 관계없이 수동으로 실행해야 하는 문제 해결에 대한 리소스 태그(하나 이상의 태그 페어, 쉼표로 구분)를 지정합니다.

예를 들어 모든 비프로덕션 리소스에 대해 자동 문제 해결을 활성화하고 프로덕션 리소스에 대해 수동 문제 해결을 적용하려면 구성을 다음과 같이 설정할 수 있습니다.

```
"execution-mode": "Conditional",
"automated-for-tagged-only": "Environment=Non-Production",
>manual-for-tagged-only": "Environment=Production",
```

리소스에 이전 구성이 설정된 경우 문제 해결 동작이 다음과 같은지 확인합니다.

- 'Environment=Non-Production'으로 태그가 지정된 리소스는 자동으로 수정됩니다.
- 'Environment=Production'으로 태그가 지정된 리소스는 수정을 위해 수동 개입이 필요합니다.
- '환경' 태그가 없는 리소스는 기본 실행 모드(이 경우 '조건부')를 따릅니다. 따라서 나머지 리소스에 대해서는 아무런 조치도 취하지 않습니다.)

구성에 대한 추가 지원은 Cloud Architect에 문의하십시오.

리소스 재정의의 태그를 사용하여 문제 해결 사용자 지정

리소스 재정의의 태그를 사용하면 태그에 관계없이 개별 리소스의 문제 해결 동작을 사용자 지정할 수 있습니다. 리소스에 특정 태그를 추가하면 해당 리소스의 기본 실행 모드와 Trusted Advisor 검사를 재정의할 수 있습니다. 리소스 재정의의 태그는 기본 구성 및 리소스 태그 지정 설정보다 우선합니다. 따라서 리소스 재정의의 태그를 사용하여 리소스에 대해 기본 실행 모드를 자동, 수동 또는 조건부로 설정하면 기본 실행 모드와 리소스 태그 지정 구성을 재정의합니다.

리소스의 실행 모드를 재정의하려면 다음 단계를 완료합니다.

1. 문제 해결 구성을 재정의할 리소스를 식별합니다.
2. 재정의하려는 Trusted Advisor 검사의 검사 ID를 확인합니다. 에서 지원되는 검사에 대한 Trusted Advisor 검사 IDs 찾을 수 있습니다 [Trusted Advisor Trusted Remediator에서 지원하는 검사](#).
3. 태그 | [업데이트 또는 태그](#) | [대량 업데이트](#) 변경 유형을 사용하여 다음 키와 값을 사용하여 리소스에 태그를 추가합니다.

- 태그 키: TR-*Trusted Advisor check ID*-Execution-Mode (대소문자 구분)

앞의 태그 키 예제에서 재정의하려는 Trusted Advisor 검사의 고유 식별로 Trusted Advisor check ID 바꿉니다.

- 태그 값: 태그 값에 다음 값 중 하나를 사용합니다.
 - 자동: 신뢰할 수 있는 수정자는 이 Trusted Advisor 검사에 대한 리소스를 자동으로 수정합니다.
 - 수동: 리소스에 대해 OpsItem이 생성되지만 수정이 자동으로 수행되지 않습니다. 자동으로 사용하여 문제 해결을 검토하고 실행합니다. 자세한 내용은 [신뢰할 수 있는 수정자에서 문제 해결 작업](#) 단원을 참조하십시오.
 - 비활성: 이 리소스 및 지정된 Trusted Advisor 검사에 대해 수정 및 OpsItem 생성이 수행되지 않습니다.

예를 들어 Trusted Advisor 검사 ID가 인 Amazon EBS 볼륨을 자동으로 해결하려면 EBS 볼륨에 태그를 DAVU99Dc4C 추가합니다. 태그 키는 TR-DAVU99Dc4C-Execution-Mode이고 태그 값은 입니다 Automated.

다음은 태그 섹션을 보여주는 콘솔의 예입니다.

실행 모드 결정 워크플로

리소스 및 각 Trusted Advisor 검사에 대한 실행 모드를 구성하는 데는 여러 수준이 있습니다. 다음 다이어그램은 Trusted Remediator가 구성에 따라 사용할 실행 모드를 결정하는 방법을 보여줍니다.

문제 해결 자습서 구성

다음 자습서에서는 신뢰할 수 있는 문제 해결자에서 일반적인 문제 해결을 생성하는 예를 제공합니다.

모든 리소스를 수동으로 수정

이 예제에서는 Trusted Advisor 검사 ID가 DAvU99Dc4C(사용되지 않은 Amazon EBS 볼륨)인 모든 Amazon EBS 볼륨에 대한 수동 문제 해결을 구성합니다.

검사 ID DAvU99Dc4C를 사용하여 Amazon EBS 볼륨에 대한 수동 문제 해결 구성

1. 수정 구성|업데이트, 변경 유형을 사용하여 구성 업데이트를 요청합니다.
2. 다음 파라미터를 입력합니다.
 - CheckIds: DAvU99Dc4C
 - ExecutionMode: 수동

Note

단일 요청으로 여러 검사를 구성할 수 있습니다. 동일한 구성이 필요한 검사의 경우 CheckIds 파라미터에 여러 검사 IDs를 포함합니다. CheckIds 다른 구성이 필요한 검사의 경우 새 RemediationConfiguration 객체를 생성합니다.

3. RFC를 제출합니다.

선택한 리소스를 제외한 모든 리소스를 자동으로 해결합니다.

이 예제에서는 Trusted Advisor 검사 ID가 DAvU99Dc4C(사용되지 않은 Amazon EBS 볼륨)인 모든 Amazon EBS 볼륨에 대해 자동 문제 해결을 구성합니다. 단, 수정되지 않는 지정된 볼륨(비활성으로 지정됨).

선택한 비활성 리소스를 제외하고 검사 ID가 DAvU99Dc4C인 Amazon EBS 볼륨에 대한 자동 문제 해결 구성

1. 선택한 Amazon EBS 볼륨에 대한 자동 문제 해결 재정의:

[태그 | 업데이트](#) 또는 [태그 | 대량 업데이트](#) 변경 유형을 사용하여 자동 문제 해결에서 제외할 볼륨에 대해 다음 태그를 적용합니다.

- 키: TR-DAvU99Dc4C-Execution-Mode
- 값: 비활성

2. 수정 구성|업데이트 변경 유형을 사용하여 구성 업데이트를 요청합니다.

3. 다음 파라미터를 입력합니다.

- CheckIds: DAvU99Dc4C
- ExecutionMode: 자동

4. RFC를 제출합니다.

태그가 지정된 리소스 자동 수정

이 예제에서는 Trusted Advisor 검사 ID가 DAvU99Dc4C(사용되지 않은 Amazon EBS 볼륨)인 태그 Stage=NonProd가 있는 모든 Amazon EBS 볼륨에 대해 자동 문제 해결을 구성합니다. 이 태그가 없는 다른 모든 리소스는 수정되지 않습니다.

검사 ID DAvU99Dc4C의 태그를 사용하여 Amazon EBS 볼륨에 **Stage=NonProd** 대한 자동 문제 해결 구성

1. [수정 구성 | 업데이트](#), 변경 유형을 사용하여 구성 업데이트를 요청합니다.

2. 다음 파라미터를 입력합니다.

- CheckIds: DAvU99Dc4C
- ExecutionMode: 조건부
- AutomatedForTaggedOnly: {"Stage":"NonProd"}

Note

AutomatedForTaggedOnly 파라미터에 지정된 값은 이전에 구성된 값을 재정의합니다. 기존 태그를 유지하려면 새 값에 포함시킵니다.

3. RFC를 제출합니다.

구성을 기본값으로 재설정

이 예제에서는 검사 Hs4Ma3G104에 대한 태그automated-for-tagged-only 구성을 제거합니다. 이전에 적용된 태그 구성을 제거하려면 AutomatedForTaggedOnly 파라미터 값을 {}로 설정합니다.

확인 Hs4Ma3G104의 구성을 기본값으로 재설정

1. [수정 구성](#) 변경 유형 업데이트를 사용하여 구성 업데이트를 요청합니다.
2. 다음 파라미터를 입력합니다.
 - CheckIds: Hs4Ma3G104
 - ExecutionMode: 현재 사용된 값을 입력합니다.
 - AutomatedForTaggedOnly: {}
3. RFC를 제출합니다.

신뢰할 수 있는 수정자에서 문제 해결 작업

신뢰할 수 있는 해결 방법에서 문제 해결 추적

OpsItems 문제 해결을 추적하려면 다음 단계를 완료하세요.

1. <https://console.aws.amazon.com/systems-manager/> AWS Systems Manager 콘솔을 엽니다.
2. 작업 관리, OpsCenter를 선택합니다.
3. (선택 사항) 목록에 신뢰할 수 있는 수정자 OpsItem만 포함하도록 Source=Trusted OpsItems를 기준으로 목록을 필터링합니다.

다음은 Source=Trusted Remediator로 필터링된 OpsCenter 화면의 예입니다.

Note

OpsItems 보는 것 외에도 AMS S3 버킷에서 문제 해결 로그를 볼 수 있습니다. OpsCenter 자세한 내용은 [신뢰할 수 있는 수정자의 수정 로그](#) 단원을 참조하십시오.

신뢰할 수 있는 수정자에서 수동 수정 실행

Trusted Remediator는 수동 문제 해결을 위해 구성된 검사에 대한 OpsItems 생성합니다. 이러한 검사를 검토하고 해결 프로세스를 수동으로 시작해야 합니다.

OpsItem을 수동으로 수정하려면 다음 단계를 완료하세요.

1. <https://console.aws.amazon.com/systems-manager/> AWS Systems Manager 콘솔을 엽니다.
2. 작업 관리, OpsCenter를 선택합니다.
3. (선택 사항) 목록에 신뢰할 수 있는 수정자 OpsItem만 포함하도록 Source=Trusted OpsItems를 기준으로 목록을 필터링합니다.
4. 검토하려는 OpsItem을 선택합니다.
5. OpsItem의 운영 데이터를 검토합니다. 운영 데이터에는 다음 항목이 포함됩니다.
 - trustedAdvisorCheckCategory: Trusted Advisor 검사 ID의 범주입니다. 예: 내결함성
 - trustedAdvisorCheckId: 고유한 Trusted Advisor 검사 ID입니다.
 - trustedAdvisorCheckMetadata: 리소스 ID를 포함한 리소스 메타데이터입니다.
 - trustedAdvisorCheckName: Trusted Advisor 검사의 이름입니다.
 - trustedAdvisorCheckStatus: 리소스에 대해 감지된 Trusted Advisor 검사의 상태입니다.
 - trustedAdvisorCheckManualRemediation: 수동 문제 해결을 위한 참조 세부 정보를 제공하는 사용자 지정 데이터입니다.
 - ManualExecutionInput: 수동 문제 해결을 실행할 때 값을 수정할 수 있는 파라미터를 정의하는 객체입니다.
 - DocumentName: 실행서의 이름(SSM 문서).
 - CustomizableParameters: 수정할 수 있는 파라미터 이름입니다.
 - DefaultInput: 수동 수정에 사용할 파라미터 이름과 값을 정의하는 객체입니다. 값은 미리 구성된 파라미터에 따라 채워집니다.
6. OpsItem을 수동으로 수정하려면 다음 단계를 완료하세요.
 - a. [신뢰할 수 있는 수정자 사용 | 조사 결과 | ct-1c7ch8z5phrjp 변경 유형 수정](#)

- b. 다음 파라미터에 대해 값을 입력합니다.
- **DocumentName**: 이어야 합니다 `AWSManagedServices-RemediateTrustedRemediatorFinding`.
 - **리전**: us-east-1 형식 AWS 리전의 입니다.
 - **파라미터**: 수동 문제 해결 파라미터를 입력합니다.
 - **OpsItemId**: Ops 항목의 ID입니다.
 - **RemediationDocumentName**: 사용할 SSM 자동화 문서의 이름입니다. 문서는 Ops 항목과 연결되어야 합니다. 여러 문서가 Ops 항목과 연결된 경우 **DocumentName**을 지정해야 합니다.
 - **RemediationParameters**: 자동화 실행을 위한 파라미터의 키/값 맵으로, 형식입니다 `{"ParameterName1\":[\"ParameterValue1\"],\"ParameterName2\":[\"ParameterValue2\"]}`. Ops 항목 `trustedAdvisorCheckManualRemediationCustomizableParameters`에 있는 파라미터만 사용할 수 있습니다. 지정하지 않으면 Ops 항목에서 파라미터와 값이 검색됩니다.
- c. **Run(실행)**을 선택합니다. 오류가 없으면 RFC가 성공적으로 생성된 페이지에 제출된 RFC 세부 정보와 초기 실행 출력이 표시됩니다.
- d. RFC 실행 진행 상황을 모니터링합니다.
- e. 실행이 완료되면 **OpsItem**이 해결됩니다. RFC가 실패한 경우의 단계를 따릅니다 [신뢰할 수 있는 해결 방법의 문제 해결](#). 추가 문제 해결 지원은 AMS에 문의하십시오.

신뢰할 수 있는 해결 방법의 문제 해결

수동 문제 해결 및 문제 해결 실패에 대한 도움이 필요하면 AMS에 문의하십시오.

문제 해결 상태 및 결과를 보려면 다음 단계를 완료하세요.

1. <https://console.aws.amazon.com/systems-manager/> AWS Systems Manager 콘솔을 엽니다.
2. 작업 관리, OpsCenter를 선택합니다.
3. (선택 사항) 목록에 신뢰할 수 있는 수정자 OpsItem만 포함하도록 **Source=Trusted OpsItems**를 기준으로 목록을 필터링합니다.
4. 검토하려는 OpsItem을 선택합니다.
5. 자동화 실행 섹션에서 문서 이름, 상태 및 결과를 검토합니다.
6. 다음과 같은 일반적인 자동화 실패를 검토합니다. 여기에 문제가 나열되지 않은 경우 CSDM에 문의하여 지원을 받으세요.

일반적인 문제 해결 오류

자동화 실행에 나열된 실행 없음

OpsItem과 연결된 실행이 없으면 잘못된 파라미터 값으로 인해 실행이 시작되지 않았음을 나타낼 수 있습니다.

문제 해결 단계

1. 운영 데이터에서 `trustedAdvisorCheckAutoRemediation` 속성 값을 검토합니다.
2. `DocumentName` 및 파라미터 값이 올바른지 확인합니다. 올바른 값을 보려면에서 SSM 파라미터를 구성하는 방법에 [신뢰할 수 있는 수정자에서 Trusted Advisor 검사 수정 구성](#) 대한 세부 정보를 검토합니다. 지원되는 검사 파라미터를 검토하려면 섹션을 참조하세요. [Trusted Advisor Trusted Remediator에서 지원하는 검사](#)
3. SSM 문서의 값이 허용된 패턴과 일치하는지 확인합니다. 문서 콘텐츠에서 파라미터 세부 정보를 보려면 런북 섹션에서 문서 이름을 선택합니다.
4. 파라미터를 검토하고 수정한 후 OpsItem을 수동으로 수정합니다. 문제 해결 단계는 섹션을 참조하세요. [신뢰할 수 있는 수정자에서 수동 수정 실행](#).
5. 이 오류가 다시 발생하지 않도록 하려면 구성에서 올바른 파라미터 값으로 문제 해결을 구성해야 합니다. 자세한 내용은 [신뢰할 수 있는 수정자에서 Trusted Advisor 검사 수정 구성](#) 섹션을 참조하세요.

자동화 실행에서 실패한 실행

문제 해결 문서에는 API를 통해 다양한 작업을 AWS 서비스 수행하는 것과 상호 작용하는 여러 단계가 포함되어 있습니다. APIs 실패의 특정 원인을 식별하려면 다음 단계를 완료하세요.

문제 해결 단계

1. 개별 실행 단계를 보려면 자동화 실행 섹션에서 실행 ID, 링크를 선택합니다. 다음은 선택한 자동화의 실행 단계를 보여주는 Systems Manager 콘솔의 예입니다.
2. 실패 상태의 단계를 선택합니다. 다음은 오류 메시지의 예입니다.
 - NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist

이 오류는 문제 해결 구성의 사전 구성된 파라미터에 잘못된 버킷 이름이 지정되었음을 나타냅니다.

이 오류를 해결하려면 올바른 버킷 이름을 사용하여 [자동화를 수동으로 실행합니다](#). 이 문제가 다시 발생하지 않도록 하려면 문제 [해결 구성을 올바른 버킷 이름으로 업데이트](#)합니다.

- DB instance my-db-instance-1 is not in available status for modification.

이 오류는 DB 인스턴스가 잘못된 상태이기 때문에 자동화가 예상대로 변경할 수 없음을 나타냅니다.

이 오류를 해결하려면 [자동화를 수동으로 실행합니다](#).

신뢰할 수 있는 수정자의 수정 로그

Trusted Remediator는 JSON 형식으로 로그를 생성하고 Amazon Simple Storage Service에 업로드합니다. 로그 파일은 AMS에서 생성하고 이름이 인 S3 버킷에 업로드됩니다 `ams-trusted-remediator-{your-account-id}-logs`. AMS는 위임된 관리자 계정에 S3 버킷을 생성합니다. 로그 파일을 QuickSight로 가져와 사용자 지정 수정 보고서를 생성할 수 있습니다.

문제 해결 항목 로그

Trusted Remediator는 문제 해결 OpsItem이 생성될 Remediation item log 때를 생성합니다. 이 로그에는 수동 문제 해결 OpsItem과 자동 문제 해결 OpsItem이 포함되어 있습니다. Remediation item log를 사용하여 모든 수정 사항의 개요를 추적할 수 있습니다.

Compute Optimizer 권장 사항에 대한 문제 해결 항목 로그 위치

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs/  
compute_optimizer_remediation_items/remediation creation time in yyyy-mm-dd format/10 digits epoch time or unix timestamp-Trust  
ed Advisor check ID-Resource ID.json
```

Trusted Advisor 검사를 위한 문제 해결 항목 로그 위치

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs/  
remediation_items/remediation creation time in yyyy-mm-dd format/10 digits epoch time or unix timestamp-Trust  
ed Advisor check ID-Resource ID.json
```

문제 해결 항목 로그 샘플 파일 URL

s3:///ams-trusted-remediator-111122223333-logs/
remediation_items/2023-02-06/1675660464-DAvU99Dc4C-
vol-00bd8965660b4c16d.json

Compute Optimizer 문제 해결 항목 로그 형식

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor 문제 해결 항목 로그 형식

```
{
  "TrustedAdvisorCheckID": Trusted Advisor check ID,
  "TrustedAdvisorCheckName": Trusted Advisor check name,
  "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
  "ResourceID": Resource ID,
  "RemediationTime": Remediation creation time,
  "ExecutionMode": Automated or Manual,
  "OpsItemID": OpsItem ID
}
```

Compute Optimizer 문제 해결 항목 로그 형식 샘플 콘텐츠

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor 문제 해결 항목 로그 형식 샘플 콘텐츠

```
{
  "TrustedAdvisorCheckID": "DAvU99Dc4C",
  "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
  "TrustedAdvisorCheckResultTime": 1675614749,
  "ResourceID": "vol-00bd8965660b4c16d",
  "RemediationTime": 1675660464,
  "OpsItemID": "oi-cca5df7af718"
}
```

자동 문제 해결 실행 로그, Compute Optimizer 및 Trusted Advisor

신뢰할 수 있는 수정자는 자동 SSM 문서 실행이 완료되면 Automated remediation execution log를 생성합니다. 이 로그에는 자동 문제 해결 OpsItem에 대한 SSM 실행 세부 정보만 포함되어 있습니다. 이 로그 파일을 사용하여 자동 문제 해결을 추적할 수 있습니다.

Compute Optimizer 자동 문제 해결 로그 위치

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs//
remediation_executions/*remediation creation time in yyyy-mm-dd format/10
digits epoch time or unix timestamp-Compute Optimizer recommendation
ID*.json

Trusted Advisor 자동 문제 해결 로그 위치

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs//
remediation_executions/*remediation creation time in yyyy-mm-dd format/10
digits epoch time or unix timestamp-Trusted Advisor check ID-Resource
ID*.json

Compute Optimizer 자동 문제 해결 로그 위치 예제

s3://ams-trusted-remediator-*111122223333*-logs/
remediation_executions/2025-06-26/1750908858-123456789012-compute-
optimizer-ec2-i-1235173471d2cd789.json

Trusted Advisor 자동 문제 해결 로그 위치 예제

s3://ams-trusted-remediator-*111122223333*-logs/
remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-
vol-00bd8965660b4c16d.json

자동 문제 해결 로그 형식 샘플 콘텐츠

```
{
  "OpsItemID": "oi-767c77e05301",
  "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",
  "SSMExecutionStatus": "Success"}
```

신뢰할 수 있는 해결 방법의 모범 사례

다음은 신뢰할 수 있는 수정자를 사용하는 데 도움이 되는 모범 사례입니다.

- 해결 결과에 대해 잘 모르는 경우 수동 실행 모드로 시작합니다. 때때로 처음부터 문제 해결을 위해 자동 실행을 적용하면 예상치 못한 결과가 발생할 수 있습니다.
- 문제 해결 및 OpsItems을 매주 검토하여 신뢰할 수 있는 문제 해결사 결과에 대한 인사이트를 얻습니다.
- 멤버 계정은 위임된 관리자 계정에서 구성을 상속합니다. 따라서 동일한 구성으로 여러 계정을 관리하는 데 도움이 되는 방식으로 계정을 구성하는 것이 중요합니다. 태그를 사용하여 기본 구성에서 리소스를 제외할 수 있습니다.

신뢰할 수 있는 해결사 FAQs

다음은 신뢰할 수 있는 수정자에 대해 자주 묻는 질문입니다.

Trusted Remediator란 무엇이며 어떤 이점이 있나요?

Compute Optimizer에서 규정 미준수가 식별 Trusted Advisor 되거나 권장 사항이 발행되면 Trusted Remediator는 문제 해결을 적용하거나, 수동 문제 해결을 통해 승인을 구하거나, 예정된 월간 비즈니스 검토(MBR) 중에 문제 해결을 보고하여 지정된 기본 설정에 따라 응답합니다. 문제 해결은 원하는 문제 해결 시간 또는 일정에 이루어집니다. Trusted Remediator는 Trusted Advisor 검사를 개별적으로 또는 대량으로 구성하고 수정할 수 있는 유연성과 함께 검사를 셀프 서비스하고 수행할 수 있는 기능을 제공합니다. AMS는 테스트된 문제 해결 문서 라이브러리를 통해 안전 검사를 적용하고 AWS 모범 사례를 따라 계정을 지속적으로 높입니다. 구성에서 그렇게 하도록 지정한 경우에만 알림을 받습니다. AMS 사용자는 추가 비용 없이 신뢰할 수 있는 수정자를 선택할 수 있습니다.

Trusted Remediator는 다른와 어떤 관련이 있고 어떻게 작동하나요 AWS 서비스?

기존 Enterprise Support 플랜의 일부로 Trusted Advisor 검사 및 Compute Optimizer 권장 사항에 액세스할 수 있습니다. Trusted Remediator는 및 Compute Optimizer와 Trusted Advisor 통합되어 기

존 AMS 자동화 기능을 활용합니다. 특히 AMS는 자동 문제 해결을 위해 AWS Systems Manager 자동화 문서(런북)를 사용합니다. AWS AppConfig 는 문제 해결 워크플로를 구성하는 데 사용됩니다. Systems Manager OpsCenter를 통해 현재 및 과거 수정 사항을 모두 볼 수 있습니다. 문제 해결 로그는 Amazon S3 버킷에 저장됩니다. 로그를 사용하여 QuickSight에서 사용자 지정 보고 대시보드를 가져오고 빌드할 수 있습니다.

문제 해결은 누가 구성하나요?

계정의 구성을 소유합니다. 구성 관리는 사용자의 책임입니다. 구성 변경, 지원 및 수동 문제 해결, 문제 해결 실패 문제 해결을 위해 AMS에 문의할 수도 있습니다.

SSM 자동화 문서를 설치하려면 어떻게 해야 하나요?

SSM 자동화 문서는 온보딩된 AMS 계정에 자동으로 공유됩니다.

AMS 소유 리소스도 수정되나요?

AMS 소유 리소스는 신뢰할 수 있는 수정자에서 플래그를 지정하지 않습니다. Trusted Remediator는 리소스에만 중점을 둡니다.

에서 사용할 수 있는 신뢰할 수 있는 해결 방법은 AWS 리전 무엇이며 누가 사용할 수 있습니까?

신뢰할 수 있는 수정자는 AMS Advanced 고객이 사용할 수 있습니다. 현재 지원 리전 목록은 [AWS 서비스 리전별](#) 섹션을 참조하세요.

신뢰할 수 있는 해결 방법으로 인해 리소스 드리프트가 발생하나요?

SSM 자동화 문서는 AWS API를 통해 리소스를 직접 업데이트하므로 리소스 드리프트가 발생할 수 있습니다. 태그를 사용하여 기존 CI/CD 패키지를 통해 생성된 리소스를 분리할 수 있습니다. 다른 리소스를 여전히 해결하면서 태그가 지정된 리소스를 무시하도록 신뢰할 수 있는 해결 방법을 구성할 수 있습니다.

신뢰할 수 있는 수정자를 일시 중지하거나 중지하려면 어떻게 해야 합니까?

[Management | Trusted Remediator | State | Enable or disable](#) change type을 사용하여 Trusted Remediator 서비스를 중지합니다. 동일한 변경 유형을 사용하여 신뢰할 수 있는 수정자를 다시 활성화합니다.

Trusted Remediator에서 지원하지 않는 검사를 해결하려면 어떻게 해야 하나요?

지원되지 않는 검사를 위해 OOD(운영 온디맨드)를 통해 AMS에 계속 연락할 수 있습니다. AMS는 이러한 검사를 해결하는 데 도움이 됩니다. 자세한 내용은 [온디맨드 작업을](#) 참조하세요.

Trusted Remediator는 계정에 어떤 리소스를 배포하나요?

Trusted Remediator는 Trusted Remediator 위임된 관리자 계정에 다음 리소스를 배포합니다.

- `ams-trusted-remediator-{your-account-id}-logs`이라는 Amazon S3 버킷. Trusted Remediator는 문제 해결 OpsItem이 생성될 때 Remediation item log JSON 형식으로 생성하고 로그 파일을 이 버킷에 업로드합니다.
- 지원되는 Trusted Advisor 검사 및 Compute Optimizer 권장 사항에 대한 문제 해결 구성을 보유하는 AWS AppConfig 애플리케이션입니다.

Trusted Remediator는 Trusted Remediator 멤버 계정에 리소스를 배포하지 않습니다.

로그 관리

주제

- [로그 관리란 무엇입니까?](#)
- [AMS 로깅 작동 방식](#)
- [로그 액세스](#)
- [로그 구성 사용자 지정](#)

AMS 로그 관리는 관리형 계정에서 로그의 보존을 수집, 집계 및 제어합니다. AWS 로그 관리는 계정 내에 배포된 Amazon EC2 인스턴스 및 AWS 리소스의 로그를 CloudWatch Logs로 집계합니다. 현재 로그가 집계된 서비스의 전체 목록은 [여기](#)에서 확인할 수 있습니다.

로그 관리란 무엇입니까?

로그 관리는 인스턴스, 애플리케이션 및 AWS 서비스에서 생성된 로그 이벤트를 처리하는 프로세스입니다. 이 기능은 AMS가 관리형 AWS 계정에서 생성된 로그 이벤트를 처리, 저장 및 교체하는 방법을 정의합니다. 인프라 로그는 인시던트 해결 및 시스템 감사를 지원하는 데 사용됩니다.

AMS 로깅 작동 방식

AMS 단일 계정 랜딩 존(SALZ) 로그 관리는 인스턴스 및 애플리케이션이 온보딩되거나 프로비저닝될 때 구현되는 다양한 사전 설치된 에이전트 및 도구를 사용합니다.

계정 온보딩 프로세스 중에 그리고 스택이 시작될 때 로깅이 구성됩니다.

인스턴스 및 AWS 서비스에서 생성된 AMS 다중 계정 랜딩 존(MALZ) 로그는 AMS에서 관리하는 각 계정 내에서 CloudWatch Logs 또는 Amazon Simple Storage Service(Amazon S3)에서 사용할 수 있습니다. AMS 다중 계정 랜딩 존은 개별 애플리케이션 계정에서 생성된 일부 로그의 중앙 집계 위치 역할을 하는 중앙 로깅 계정을 제공합니다.

[로그 액세스](#) 하위 섹션의 표에는 개별 계정에서 사용할 수 있는 로그와 중앙 로깅 계정에서 사용할 수 있는 로그가 설명되어 있습니다.

로그 액세스

로그에 액세스하려면 필요한 IAM 역할 중 하나가 있고 AMS 계정에 있는지 확인합니다. 그런 다음 표시된 디렉터리로 이동합니다.

Multi-Account Landing Zone (MALZ)

5개의 기본 IAM 역할을 제공하며, 각 역할은 계정 내의 모든 로그에 대한 액세스를 허용합니다(모두 앞에가 붙음AWSManagedServices).

- AdminRole
- CaseRole
- ChangeManagementRole
- ReadOnlyRole
- SecurityOpsRole

이러한 역할에 대한 액세스는 페더레이션을 통해 구성되며 각 역할은 Active Directory 도메인 내의 그룹에 매핑됩니다.

이러한 역할에 대한 자세한 내용은 섹션을 참조하세요 [AMS의 IAM 사용자 역할](#).

Single-Account Landing Zone (SALZ)

AMS 단일 계정 랜딩 존Customer_ReadOnly_Role의 기본값을 사용하면 계정 내의 모든 로그에 액세스할 수 있습니다. 로그에 대한 액세스는 Active Directory 그룹에 매핑된 AWS Identity and Access Management(IAM) 역할을 사용하여 제어됩니다.

AMS 집계 서비스 로그

각 AWS 서비스는 CloudWatch Logs 또는 Amazon S3 버킷의 특정 위치에 로깅합니다.

Note

특히 명시되지 않는 한 모든 로그 위치는 로그를 생성한 계정에 로컬이며 중앙 로깅 계정으로 집계되지 않습니다.

SALZ 및 MALZ 계정에서 기본 AMS CloudTrail 추적 이름을 찾으려면 CloudTrail용 AWS 콘솔로 이동한 다음 추적 페이지로 이동하여 AMS를 검색합니다. AMS 리소스에는 태그가 있으므로 이러한 방식으로 추적을 찾을 수 있습니다. AMS CloudTrail 태그의 예:

Environment AMSInfrastructure

로그에 액세스하려면 필요한 IAM 역할 중 하나가 있고 AMS 계정에 있는지 확인합니다. 그런 다음 표시된 디렉터리로 이동합니다.

Multi-Account Landing Zone

AMS 다중 계정 랜딩 존 집계된 서비스 로그

	서비스 이름	로그 세부 정보	로그 위치
1	Amazon Aurora	일반, 느린 쿼리 및 오류 로그.	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }
2	AWS CloudFormation (CFN)	API 호출 로깅만 해당됩니다.	AWS CloudFormation API 호출은 CloudTrail을 통해 문서화되며, CloudTrail은 로그를 CloudWatch LogGroup으로 전송한 다음 로그를 S3 버킷에 동기화합니다. 로그는 CloudWatch LogGroup에서 기본적으로 14일 동안 보존되며 S3 버킷에 무기한 보존됩니다. CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs S3 버킷 [중앙 로깅 계정에서]: aws-landing-zone-logs-ams-a {<i>account_ID</i> }-log-management- {<i>region</i>} 경로: /AWSLogs/{<i>account_ID</i> }/ CloudTrail/

	서비스 이름	로그 세부 정보	로그 위치
3	Amazon CloudFront(CloudFront)	사용자 요청 로깅. CloudFront 로깅을 명시적으로 활성화해야 합니다. 자세한 내용은 지원되는 서비스에 대한 로깅 활성화 단원을 참조하세요.	S3 버킷: <code>ams-a{account_ID}-log-management-{region}</code> 경로: <code>AWS/RedShift/{CloudFront ## ID}</code>
4	Amazon CloudWatch(CloudWatch)	API 호출 로깅만 해당됩니다.	CloudWatch LogGroup: <code>/CloudTrail/Landing-Zone-Logs</code> S3 버킷 [중앙 로깅 계정에 서]: <code>aws-landing-zone-logs-{account_ID}-{region}</code> 경로: <code>/AWSLogs/{account_ID}/CloudTrail/</code>
5	Amazon Elastic Block Store(Amazon EBS)	EBS 서비스에서는 로그를 생성하지 않습니다.	해당 사항 없음
6	Amazon Elastic Compute Cloud(Amazon EC2)	시스템 및 애플리케이션 로그. 자세한 내용은 단원을 참조하십시오 Amazon Elastic Compute Cloud(Amazon EC2) - 시스템 수준 로그 .	CloudWatch Logs: <code>/#### ID</code>
7	Amazon Elastic File System(Amazon EFS)	API 호출 로깅만 해당됩니다.	CloudWatch LogGroup: <code>/CloudTrail/Landing-Zone-Logs</code> S3 버킷 [중앙 로깅 계정에 서]: <code>aws-landing-zone-logs-{account_ID}-{region}</code> 경로: <code>/AWSLogs/{account_ID}/CloudTrail/</code>

	서비스 이름	로그 세부 정보	로그 위치
8	Elastic Load Balancing(ELB)	액세스 및 오류 로그 항목. 탄력적 로드 밸런서는 백엔드 인스턴스로 라우팅되지 않은 요청을 포함하여 전송된 모든 요청을 로깅합니다. 예를 들어 클라이언트가 잘못된 형식의 요청을 보내거나 응답할 정상 인스턴스가 없는 경우에도 요청은 계속 로깅됩니다. Elastic Load Balancing 로그 항목에 대한 자세한 내용은 섹션을 참조하세요. • Classic Load Balancer: 로그 항목에 액세스합니다. • Application Load Balancer: 로그 항목에 액세스합니다. • Network Load Balancer: 로그 항목에 액세스합니다.	API 호출 로그: CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs S3 버킷 [중앙 로깅 계정에]: aws-landing-zone-logs-{account_ID} -{region} 경로: /AWSLogs/{account_ID} /CloudTrail/ 액세스 로그: S3 버킷: mc-a{account_ID} -logs{region} 경로: aws/elbaccess
9	Amazon OpenSearch Service(OpenSearch Service)	서비스 오류 로그. OpenSearch 로깅을 명시적으로 활성화해야 합니다. 자세한 정보는 지원되는 서비스에 대한 로깅 활성화 섹션을 참조하세요.	CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs S3 버킷 [중앙 로깅 계정에]: aws-landing-zone-logs-{account_ID} -{region} 경로: /AWSLogs/{account_ID} /CloudTrail/

	서비스 이름	로그 세부 정보	로그 위치
10	Amazon ElastiCache	API 호출 로깅만 해당됩니다.	CloudWatch LogGroup: //CloudTrail/Landing-Zone-Logs
11	Amazon GuardDuty		S3 버킷 [중앙 로깅 계정에 서]: aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> }
12	Amazon Inspector		경로: /AWSLogs/{ <i>account_ID</i> }/ CloudTrail/
13	Amazon Macie		
14	Amazon Redshift	연결, 사용자 및 활동 로그. 로깅은 Redshift 클러스터 생성 CT(ct-1malj7snzxrkr)를 호출하여 Redshift 클러스터를 생성할 때 기본적으로 활성화됩니다. 자세한 내용은 데이터베이스 감사 로깅을 참조하세요.	S3 버킷: ams-a{<i>account_ID</i> }-log-management-{<i>region</i>} 경로: /AWS/RedShift/{<i>CloudFront ## ID</i> }
15	Amazon Relational Database Service(RDS)	데이터베이스 유형별 로그입니다. RDS 로깅을 명시적으로 활성화해야 합니다. 자세한 정보는 지원되는 서비스에 대한 로깅 활성화 섹션을 참조하세요. 저장 프로시저를 통해서만 MSSQL 로그에 액세스할 수 있습니다. 자세한 내용은 로그 파일 보관을 참조하세요.	CloudWatch LogGroup: /aws/rds/(##### 또는 #####)/ {<i>database_name</i> }/{<i>log_name</i>}

	서비스 이름	로그 세부 정보	로그 위치
16	Amazon S3(S3)	버킷 액세스 로그. 각 액세스 로그 레코드는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태 및 오류 코드(있는 경우)와 같은 단일 액세스 요청에 대한 세부 정보를 제공합니다. 액세스 로그 정보는 보안 및 액세스 감사에 유용할 수 있습니다. 또한 고객 기반을 이해하고 Amazon S3 청구 비용을 파악할 수 있습니다. S3 액세스 로그 항목에 대한 자세한 내용은 S3 서버 액세스 로그 형식을 참조하세요.	S3 버킷: mc-a{<i>account_ID</i> }-log-management-{<i>region</i>} 경로: /aws/s3access/{<i>bucket_name</i> } S3 버킷 [중앙 로깅 계정에서]: aws-landing-zone-s3-access-logs-{<i>account_ID</i> }-{<i>region</i>} 경로: /
17	Amazon Simple Email Service(SES)	SES API 서비스 호출.	CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs S3 버킷 [중앙 로깅 계정에서]: aws-landing-zone-logs-{<i>account_ID</i> }-{<i>region</i>} 경로: /AWSLogs/{<i>account_ID</i> }/CloudTrail/
18	Amazon Virtual Private Cloud(VPC)	VPC 흐름 데이터(VPC의 네트워크 인터페이스로 들어오고 나가는 IP 트래픽에 대한 정보).	CloudWatch LogGroup: /aws/vpcflow/{ <i>VPC_ID</i> }

	서비스 이름	로그 세부 정보	로그 위치
19	오토 스케일링	API 호출 로깅만 해당됩니다.	CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs
20	AWS Certificate Manager		S3 버킷 [중앙 로깅 계정에 서]: aws-landing-zone-logs- {<i>account_ID</i>}-{<i>region</i>} 경로: /AWSLogs/{<i>account_ID</i> }/ CloudTrail/
21	AWS CodeDeploy	인스턴스별 배포 로그입니다.	인스턴스에서
22	Config	AWS Config API 서비스 호출.	CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs S3 버킷 [중앙 로깅 계정에 서]: aws-landing-zone-logs- {<i>account_ID</i>}-{<i>region</i>} 경로: /AWSLogs/{<i>account_ID</i> }/ CloudTrail/
		AWS Config에서 추적하는 리소스 구성 변경.	S3 버킷 [중앙 로깅 계정에 서]: aws-landing-zone-logs- {<i>account_ID</i>}-{<i>region</i>} 경로: /AWSLogs/{<i>account_ID</i> }/ Config/
23	AWS Database Migration Service	데이터베이스 마이그레이션 로그. 자세한 내용은 AWS Database Migration Service의 로그 관리 소개를 참조하세요.	데이터베이스 마이그레이션 콘솔

	서비스 이름	로그 세부 정보	로그 위치
24	AWS Direct Connect(DX)	API 호출 로깅만 해당됩니다.	CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs
25	AWS Glacier		S3 버킷 [중앙 로깅 계정에 서]: aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> }
26	AWS IAM(IAM)		
27	AWS Key Management Service		경로: /AWSLogs/{ <i>account_ID</i> }/ CloudTrail/
28	AWS Management Console(콘솔 또는 AWS 콘솔)		
29	AWS Simple Notification Service(SNS)		
30	AWS Simple Queueing Service(SQS)		

Single-Account Landing Zone

AMS 단일 계정 랜딩 존 집계된 서비스 로그

	서비스 이름	로그 세부 정보	로그 위치
1	Amazon Aurora	일반, 느린 쿼리 및 오류 로그.	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/ { <i>log_name</i> }
2	Amazon CloudForm	API 호출 로깅만 해당됩니다.	CloudFormation API 호출은 CloudTrail을 통해 문서화되며,

	서비스 이름	로그 세부 정보	로그 위치
	ation(CloudFormation 또는 CFN)		CloudTrail은 로그를 CloudWatch LogGroup으로 전송한 다음 로그를 S3 버킷에 동기화합니다. CloudWatch LogGroup: /aws/ams/cloudtrail S3 버킷: <code>ams-a{<i>account_ID</i> }-log-management-{<i>region</i>}</code>
3	Amazon CloudFront(CloudFront)	사용자 요청 로깅. CloudFront 로깅을 명시적으로 활성화해야 합니다. 자세한 정보는 지원되는 서비스에 대한 로깅 활성화 섹션을 참조하세요.	S3 버킷: <code>ams-a{<i>account_ID</i> }-log-management-{<i>region</i>}</code> 경로: <code>AWS/RedShift/{<i>CloudFront_distribution_ID</i> }</code>
4	Amazon CloudWatch(CloudWatch)	API 호출 로깅만 해당됩니다.	CloudWatch LogGroup: /aws/ams/cloudtrail
5	Amazon Elastic Block Store(EBS)	EBS 서비스에서는 로그를 생성하지 않습니다.	해당 사항 없음
6	Amazon Elastic Compute Cloud(EC2)	시스템 및 애플리케이션 로그. 자세한 내용은 단원을 참조하십시오 Amazon Elastic Compute Cloud(Amazon EC2) - 시스템 수준 로그 .	CloudWatch Logs: <code>/i{<i>instance_ID</i> }</code>
7	Amazon Elastic File System(Amazon EFS)	API 호출 로깅만 해당됩니다.	CloudWatch LogGroup: /aws/ams/cloudtrail

	서비스 이름	로그 세부 정보	로그 위치
8	Elastic Load Balancing(ELB)	액세스 및 오류 로그 항목. 탄력적 로드 밸런서는 백엔드 인스턴스로 라우팅되지 않은 요청을 포함하여 전송된 모든 요청을 로깅합니다. 예를 들어 클라이언트가 잘못된 형식의 요청을 보내거나 응답할 정상 인스턴스가 없는 경우에도 요청은 계속 로깅됩니다. 탄력적 로드 밸런서 로그 항목에 대한 자세한 내용은 섹션을 참조하세요. • Classic Load Balancer: 로그 항목에 액세스합니다. • Application Load Balancer: 로그 항목에 액세스합니다. • Network Load Balancer: 로그 항목에 액세스합니다.	CloudWatch LogGroup: /aws/ams/cloudtrail S3 버킷: mc-a{<i>account_ID</i> }-logs-{<i>region</i>} 경로: aws/elbaccess
9	Amazon OpenSearch Service(OpenSearch Service)	서비스 오류 로그. OpenSearch 로깅을 명시적으로 활성화해야 합니다. 자세한 정보는 지원되는 서비스에 대한 로깅 활성화 섹션을 참조하세요.	CloudWatch LogGroup: /aws/ams/cloudtrail
10	Amazon ElastiCache	API 호출 로깅만 해당됩니다.	CloudWatch LogGroup: /aws/ams/cloudtrail
11	Amazon GuardDuty		
12	Amazon Inspector		

	서비스 이름	로그 세부 정보	로그 위치
13	Amazon Macie		
14	Amazon Redshift	연결, 사용자 및 활동 로그. 로깅은 Redshift 클러스터 생성 CT(ct-1malj7snzxrkr)를 호출하여 Redshift 클러스터를 생성할 때 기본적으로 활성화됩니다. 자세한 내용은 데이터베이스 감사 로깅을 참조하세요.	S3 버킷: <code>ams-a{<i>account_ID</i> }-log-management-{<i>region</i>}</code> 경로: <code>/AWS/RedShift/{<i>CloudFront_Distribution_ID</i> }</code>
15	Amazon Relational Database Service(RDS)	데이터베이스 유형별 로그입니다. RDS 로깅을 명시적으로 활성화해야 합니다. 자세한 정보는 지원되는 서비스에 대한 로깅 활성화 섹션을 참조하세요. 저장 프로시저를 통해서만 MSSQL 로그에 액세스할 수 있습니다. 자세한 내용은 로그 파일 보관을 참조하세요.	CloudWatch LogGroup: <code>/aws/rds/(instance cluster)/{database name}/{log name}</code>

	서비스 이름	로그 세부 정보	로그 위치
16	Amazon S3(S3)	버킷 액세스 로그. 각 액세스 로그 레코드는 요청자, 버킷 이름, 요청 시간, 요청 작업, 응답 상태 및 오류 코드(있는 경우)와 같은 단일 액세스 요청에 대한 세부 정보를 제공합니다. 액세스 로그 정보는 보안 및 액세스 감사에 유용할 수 있으며, 고객 기반에 대해 알아보고 Amazon S3 청구서를 이해하는 데도 도움이 될 수 있습니다. S3 액세스 로그 항목에 대한 자세한 내용은 S3 서버 액세스 로그 형식을 참조하세요.	S3 버킷: mc-a{<i>account_ID</i> }-log-management-{<i>region</i>} 경로: /aws/s3access/{<i>bucket_name</i> }
17	Amazon Simple Email Service(SES)	SES API 서비스 호출.	CloudWatch LogGroup: /aws/ams/cloudtrail S3 버킷: ams-a{<i>account_ID</i> }-log-management-{<i>region</i>} 경로: AWS/CloudTrail/AWSLogs/{<i>account_ID</i> }/CloudTrail/{<i>region</i>}
18	Amazon Virtual Private Cloud(VPC)	VPC 흐름 데이터(VPC의 네트워크 인터페이스로 들어오고 나가는 IP 트래픽에 대한 정보).	CloudWatch LogGroup: /aws/vpcflow/{vpc_id}
19	오토 스케일링	API 호출 로깅만 해당됩니다.	CloudWatch LogGroup: /aws/ams/cloudtrail
20	AWS Certificate Manager		
21	AWS CodeDeploy	인스턴스별 배포 로그입니다.	인스턴스에서

	서비스 이름	로그 세부 정보	로그 위치
22	Config	AWS Config API 서비스 호출.	CloudWatch LogGroup: /aws/ams/cloudtrail S3 버킷: ams-a{ <i>account_ID</i> }-log-management-{ <i>region</i> } 경로: AWS/CloudTrail/AWSLogs/{ <i>account_ID</i> }/CloudTrail/{ <i>region</i> }
23	AWS Database Migration Service	데이터베이스 마이그레이션 로그. 자세한 내용은 AWS Database Migration Service의 로그 관리 소개 를 참조하세요.	데이터베이스 마이그레이션 콘솔
24	AWS Direct Connect(DX)	API 호출 로깅만 해당됩니다.	CloudWatch LogGroup: /aws/ams/cloudtrail
25	AWS Glacier		
26	AWS IAM(IAM)		
27	AWS Key Management Service		
28	AWS Management Console(콘솔 또는 AWS 콘솔)		
29	AWS Simple Notification Service(SNS)		

	서비스 이름	로그 세부 정보	로그 위치
30	AWS Simple Queueing Service(SQS)		

AMS 공유 서비스 로그

다음 표에서는 계정의 AMS 공유 서비스에 대한 로그와 로그 위치를 설명합니다.

로그에 액세스하려면 필요한 IAM 역할 중 하나가 있고 AMS 계정에 있는지 확인합니다. 그런 다음 표시된 디렉터리로 이동합니다.

AMS 단일 계정 랜딩 존 공유 서비스 로깅

	공유 서비스 이름	로그 세부 정보	로그 위치
1	접속 호스트	접속 호스트에 액세스하는 사용자에게 대한 정보입니다.	Linux Bastions: CloudWatch Logs: <code>/{{instance id}}/var/log/secure</code> CloudWatch Logs: <code>/{{instance id}}/var/log/audit/audit.log</code> Windows Bastions: CloudWatch Logs: <code>/{{instance id}}/SecurityEventLog</code>
2	관리 호스트	계정 내 자동 액세스 관리 작업을 지원하는 스크립트의 출력입니다.	CloudWatch Logs: <code>/{{instance id}}/ApplicationEventLog</code>
4	EPS 호스트(DSM)	Deep Security Management 플랫폼에 인스턴스를 등록하는 방법에 대한 정보입니다.	CloudWatch Logs: <code>/{{instance id}}/var/log/DSM.log</code>

	공유 서비스 이름	로그 세부 정보	로그 위치
5	디렉터리 서비스	계정 디렉터리 내의 계정 로그인, 계정 관리, 세부 추적, 객체 액세스, 정책 변경 및 권한 사용에 대한 정보입니다. 디렉터리 서비스 로깅을 명시적으로 활성화해야 합니다. 자세한 내용은 지원되는 서비스에 대한 로깅 활성화 단원을 참조하세요.	CloudWatch Logs: /aws/directoryservice/{directory id}-{directory dns name}
6	Lambda	계정 내 자동화된 운영 작업을 지원하는 다양한 Lambda의 출력입니다.	CloudWatch Logs: /aws/lambda/{lambda name}

AMS 다중 계정 랜딩 존 공유 서비스 로깅

	공유 서비스 이름	로그 세부 정보	로그 위치
1	Bastions	인스턴스 로그인 및 인증 실패의 출력입니다.	Linux Bastions CloudWatch Logs: / <i>{instance_ID}</i> /var/log/secure.log Windows Bastions CloudWatch Logs: / <i>{instance_ID}</i> /SecurityEventLog
2	관리 호스트	계정 내 자동 액세스 관리 작업을 지원하는 스크립트의 출력입니다.	CloudWatch Logs: / <i>{instance_ID}</i> /ApplicationEventLog
3	EPS 호스트(DSM)	Deep Security Management 플랫폼에 인스턴스를 등록하는 방법에 대한 정보입니다.	CloudWatch Logs: / <i>{instance_ID}</i> /var/log/DSM.log

	공유 서비스 이름	로그 세부 정보	로그 위치
4	디렉터리 서비스	계정 디렉터리 내의 계정 로그인, 계정 관리, 세부 추적, 객체 액세스, 정책 변경 및 권한 사용에 대한 정보입니다. 디렉터리 서비스 로깅을 명시적으로 활성화해야 합니다. 자세한 내용은 지원되는 서비스에 대한 로깅 활성화 단원을 참조하세요.	CloudWatch Logs: /aws/directoryservice/{ <i>directory_ID</i> }{ <i>directory_DNS_name</i> }
5	Lambda	계정 내 자동화된 운영 작업을 지원하는 다양한 Lambda의 출력입니다.	CloudWatch Logs: /aws/lambda/{ <i>Lambda_name</i> }

Amazon Elastic Compute Cloud(Amazon EC2) - 시스템 수준 로그

인스턴스 로그는 인스턴스에서 실행되는 CloudWatch Logs 에이전트에 의해 수집되며 인스턴스와 동일한 이름의 CloudWatch Log 그룹을 통해 액세스할 수 있습니다. 예를 들어 인스턴스 ID가 i-0123456789abcdef0이고 로그 파일 이름이 /var/log/messages인 경우 로그 그룹은 i-0123456789abcdef0이고 로그 스트림 /var/log/messages입니다.

또한 [AMS 집계 서비스 로그](#) 섹션도 참조하세요.

로그에 액세스하려면 필요한 IAM 역할 중 하나가 있고 AMS 계정에 있는지 확인합니다. 그런 다음 표시된 디렉터리로 이동합니다.

Note

다음 로그는 기본적으로 수집됩니다.

Amazon Linux / Red Hat Linux / Centos Linux / Ubuntu / SUSE Linux

로그 파일/로그 스트림

```
/var/log/amazon/ssm/amazon-ssm-agent.log
```

```
/var/log/amazon/ssm/errors.log
/var/log/audit/audit.log
/var/log/cloud-init-output.log
/var/log/cfn-init.log
/var/log/cfn-init-cmd.log
/var/log/cloud-init.log (Amazon Linux 1 / Amazon Linux 2 only)
/var/log/cron
/var/log/dnf.log
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
/var/log/yum.log
/var/log/aws/ams/bootstrap.log
/var/log/aws/ams/build.log
/var/log/syslog
/var/log/dpkg.log
/var/log/auth.log
/var/log/zypper.log
```

Note

Amazon Linux 2023용 로그에 액세스하는 방법에 대한 자세한 내용은 [EC2 Amazon Linux 2023 인스턴스에서 /var/log 디렉터리에 로그가 누락된 이유는 무엇인가요?](#)를 참조하세요.

Windows

로그 파일/로그 스트림

```
SecurityEventLog
SystemEventLog
AmazonSSMAgentLog
MicrosoftWindowsAppLockerMSIAndScriptEventLog
MicrosoftWindowsAppLockerEXEAndDLLEventLog
AmazonCloudWatchAgentLog
EC2ConfigServiceEventLog (Windows Server 2012 R2 Only)
ApplicationEventLog
AmazonCloudFormationLog
MicrosoftWindowsGroupPolicyOperationalEventLog
AmazonSSMErrorLog
```

Splunk와 통합

AMS는 Splunk와 같은 고객 로그 분석 서비스에 대한 AWS Lambda 기반 푸시를 지원합니다.

AMS는 Amazon Web 서비스용 Splunk 추가 기능을 활용하여 AWS 데이터를 Splunk로 스트리밍할 수 있습니다. [하드웨어 및 소프트웨어 요구 사항을](#) 참조하세요.

이 Splunk 블로그 게시물 [How to stream AWS CloudWatch Logs to Splunk\(힌트: 생각보다 쉬움\)](#)를 [참조하세요](#). CloudWatch 로그 스트리밍은 AMS 고객에게 기본적으로 활성화되어 있고 AMS가 AWS Lambda 함수를 구성하기 때문에 Splunk HTTP Event Collector(HEC) 입력을 구성하고 추가 기능에 대한 요청을 AMS에 제출해야 합니다.

데이터 입력 설정은 다음과 같습니다.

로그 구성 사용자 지정

CloudWatch 로그에 대한 로그 데이터 보존을 변경하고 추가 AWS 서비스에 대한 로깅을 활성화할 수 있습니다.

CloudWatch 로그 보존 변경

CloudWatch 로그에 대한 로그 데이터 보존 설정을 변경할 수 있습니다. 기본적으로 로그는 무기한으로 저장되고 만료 기간이 없습니다. 로그 그룹별로 보존 정책을 조정할 수 있고 무기한 보존 유지 또는 10년 및 하루 중 보존 기간을 선택합니다. AMS에서 허용되는 최소 보존 기간을 보려면 AWS Artifact를 통해 제공되는 AMS 기술 표준 문서를 참조하세요. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 [AWS 아티팩트 시작하기로](#) 이동합니다.

CloudWatch Logs 로그 보존 기능은 보존 정책에 따라 스트림의 로그 이벤트를 삭제합니다. 로그 스트림 또는 로그 그룹은 삭제되지 않습니다. 일반적인 내용은 Amazon CloudWatch Logs 사용 설명서 [Amazon CloudWatch Logs란 무엇입니까?](#)를 참조하세요.

로그 보존 기간을 사용자 지정하는 방법에 대한 자세한 내용은 [CloudWatch Logs의 로그 데이터 보존 변경을 참조하세요](#).

지원되는 서비스에 대한 로깅 활성화

일부 서비스에는 기본적으로 로깅이 활성화되어 있지 않으므로 명시적으로 활성화해야 합니다.

CloudFront, OpenSearch, Amazon RDS 및 Route53에 대한 로깅을 활성화하려면 다음 값으로 관리 | 기타 | 기타 | 변경 유형 생성(ct-1e1xtak34nx76)을 사용하여 RFC를 제출하고 ### 적절하게 바꿉니다.

Subject: Enable logging for *SERVICE_NAME*

Description: Service ARN: *SERVICE_ARN*

보안 관리

AWS Managed Services(AMS) 보안 관리는 AMS가 조직의 자산을 식별하고 해당 자산을 보호하기 위한 정책 및 절차를 구현하는 프로세스입니다.

Note

이제 AMS에는 인증서 요청을 제출하는 데 사용할 수 있는 변경 유형(CT), 배포 | 고급 스택 구성 요소 | 추가 SANs 있는 ACM AWS Certificate Manager 인증서 | 생성(ct-3l14e139i5p50)이 있습니다. 자세한 내용은 [AWS::CertificateManager::Certificate](#)를 참조하세요. 이 CT는 추가 주체 대체 이름(SAN)을 생성합니다.

일반적인 AWS 보안을 더 잘 이해하려면 [보안, 자격 증명 및 규정 준수 모범 사례를 참조하세요](#).

AMS는 다음과 같이 보안 위험을 분류합니다.

- 멀웨어 완화 프로세스에서 처리하는 멀웨어 방지에서 탐지된 알려진 위험.
- 보안 이벤트 관리 프로세스가 처리하는 액세스 위반을 포함한 보안 이벤트입니다.

주제

- [AMS의 데이터 보호](#)
- [자격 증명 및 액세스 관리](#)
- [AMS의 보안 인시던트 대응](#)
- [AMS Advanced의 변경 요청 보안 검토](#)

AMS의 데이터 보호

AMS는 Amazon GuardDuty, Amazon Macie(선택 사항) 및 기타 내부 독점 도구 및 프로세스와 같은 네이티브 AWS 서비스를 활용하여 관리형 계정을 지속적으로 모니터링합니다. 경보가 트리거된 후 AMS는 경보에 대한 초기 분류 및 대응을 담당합니다. 대응 프로세스는 NIST 표준을 기반으로 합니다. AMS는 보안 인시던트 대응 시뮬레이션을 사용하여 대응 프로세스를 정기적으로 테스트하여 워크플로를 기존 고객 보안 대응 프로그램에 맞게 조정합니다.

AMS가 AWS 또는 보안 정책에 대한 위반 또는 임박한 위반 위험을 감지하면 영향을 받는 리소스 및 구성 관련 변경 사항을 포함한 정보를 수집합니다. AMS는 모든 관리형 계정에서 모니터링 대시보드, 인

시던트 대기열 및 서비스 요청을 적극적으로 검토하고 조사하는 전담 운영자와 함께 연중무휴 follow-the-sun 지원을 제공합니다. AMS는 보안 전문가와 조사하여 활동을 분석하고 계정에 나열된 보안 에스컬레이션 연락처를 통해 사용자에게 알립니다.

조사 결과에 따라 AMS는 사전에 고객과 소통합니다. 활동이 무단이거나 의심스러운 경우 AMS는 사용자와 협력하여 문제를 조사 및 해결하거나 억제합니다. AMS가 조치를 취하기 전에 영향을 확인해야 하는 GuardDuty에서 생성된 특정 결과 유형이 있습니다. 예를 들어 GuardDuty 결과 유형 UnauthorizedAccess:IAMUser/ConsoleLogin은 사용자 중 한 명이 비정상적인 위치에서 로그인했음을 나타냅니다. AMS는 사용자에게 알리고이 동작이 합법적인지 확인하기 위해 결과를 검토하도록 요청합니다.

Amazon Macie

AWS Managed Services에서는 Macie를 사용하여 개인 건강 정보(PHI), 개인 식별 정보(PII) 및 금융 데이터와 같은 중요 데이터의 대규모 종합 목록을 탐지할 것을 권장합니다.

Macie는 모든 Amazon S3 버킷에서 정기적으로 실행되도록 구성하여 시간이 지남에 따라 버킷 내의 새 객체 또는 수정된 객체에 대한 평가를 자동화할 수 있습니다. 보안 조사 결과가 생성되면 AMS는 사용자에게 이를 알리고 사용자와 협력하여 필요에 따라 문제를 해결합니다.

자세한 내용은 [Amazon Macie 조사 결과 분석을 참조하세요](#).

Amazon Macie 보안

Macie는 AWS에 저장된 민감한 데이터를 자동으로 검색, 분류 및 보호하여 데이터 손실을 방지하는 데 도움이 되는 인공 지능/AI 기반 보안 서비스입니다. Macie는 기계 학습을 사용하여 개인 식별 정보(PII) 또는 지적 재산과 같은 민감한 데이터를 인식하고, 비즈니스 가치를 할당하고,이 데이터가 저장되는 위치와 조직에서 사용되는 방식에 대한 가시성을 제공합니다. Macie는 데이터 액세스 활동에 이상이 있는지 지속적으로 모니터링하고 무단 액세스 또는 의도하지 않은 데이터 유출 위험을 감지하면 알림을 전송합니다. Macie 서비스는 Amazon S3 및 AWS CloudTrail 데이터 소스를 지원합니다.

AMS는 Macie의 알림을 지속적으로 모니터링하고, 알림을 받으면 리소스와 계정을 보호하기 위한 빠른 조치를 취합니다. AMS가 지원하는 서비스 목록에 Macie를 추가하면 이제 지침에 따라 모든 계정에서 Macie를 활성화하고 구성할 책임도 있습니다. Macie 알림 및 작업이 AWS 콘솔 또는 지원되는 통합에서 펼쳐질 때 해당 알림을 볼 수 있습니다. 계정 온보딩 중에 PII를 저장하는 데 사용하는 계정을 표시할 수 있습니다. PII가 있는 모든 새 계정의 경우 Macie를 사용하는 것이 좋습니다. PII가 있는 기존 계정의 경우 문의하면 계정에서 해당 계정을 엮습니다. 따라서 추가 보호 계층을 사용할 수 있으며 AMS에서 관리하는 AWS 환경에서 Macie의 모든 이점을 누릴 수 있습니다.

AMS Macie FAQs

- 모든 AMS 계정에 Trend Micro 및 GuardDuty가 활성화된 경우 Macie가 필요한 이유는 무엇입니까?

Macie는 보유한 데이터, 데이터가 비즈니스에 미치는 가치, 해당 데이터에 대한 액세스와 관련된 동작을 분류하는 데 도움이 되므로 Amazon S3에서 데이터를 보호할 수 있습니다. Amazon GuardDuty는 위협 행위자 정찰, 인스턴스 문제 및 문제가 있는 계정 활동과 같은 위협을 식별하는 데 도움을 주어 AWS 계정, 워크로드 및 데이터를 광범위하게 보호합니다. 두 서비스 모두 사용자 동작 분석, 기계 학습 및 이상 탐지를 통합하여 각 범주에서 위협을 탐지합니다. Trend Micro는 PII 및 위협을 식별하는 데 중점을 두지 않습니다.

- AMS 계정에서 Macie를 켜려면 어떻게 해야 하나요?

계정에 PII/PHI가 저장되어 있거나 저장하려는 경우 CSDM에 문의하거나 서비스 요청을 제기하여 AMS에서 관리하는 신규 또는 기존 계정에 Macie를 활성화합니다.

- AMS 계정에서 Macie를 활성화하면 어떤 비용이 발생하나요?

Macie 요금은 Amazon Elastic Compute Cloud(Amazon EC2)와 같은 다른 서비스와 유사한 AMS에서 작동합니다. 사용량에 따라 Amazon Macie에 대해 비용을 지불하고 SLAs에 따라 AMS 상승을 지불합니다. Macie 요금은 사용량을 기준으로 합니다. AWS CloudTrail 이벤트 및 [Amazon S3 스토리지를 기준으로 측정된 Amazon Macie 요금](#)을 참조하세요. Amazon S3 Macie 요금은 Amazon S3 버킷에 추가된 증분 데이터를 기반으로 청구되므로 활성화 후 두 번째 달부터 일반화되는 경향이 있습니다.

Macie에 대한 자세한 내용은 [Amazon Macie](#)를 참조하세요.

GuardDuty

GuardDuty는 악성 IP 주소 및 도메인 목록과 같은 위협 인텔리전스 피드와 기계 학습을 사용하여 AWS 환경 내에서 예기치 않고 잠재적으로 승인되지 않은 악의적인 활동을 식별하는 지속적인 보안 모니터링 서비스입니다. 여기에는 권한 에스컬레이션, 노출된 자격 증명 사용, 악성 IP 주소 또는 도메인과의 통신과 같은 문제가 포함될 수 있습니다. 또한 GuardDuty는 Amazon Web Services 계정 액세스 동작에서 사용된 적이 없는 리전에 배포된 인스턴스와 같은 무단 인프라 배포 또는 암호 강도를 줄이기 위한 암호 정책 변경과 같은 비정상적인 API 호출과 같은 손상 징후가 있는지 모니터링합니다. 자세한 내용은 [GuardDuty 사용 설명서](#)를 참조하세요.

GuardDuty 결과를 보고 분석하려면 다음 절차를 사용합니다.

1. [GuardDuty 콘솔](#)을 엽니다.
2. 조사 결과를 선택한 다음 특정 조사 결과를 선택하여 세부 정보를 봅니다. 각 결과에 대한 세부 정보는 결과 유형, 관련된 리소스 및 활동의 특성에 따라 달라집니다.

사용 가능한 결과 필드에 대한 자세한 내용은 [GuardDuty 결과 세부](#) 정보를 참조하세요.

GuardDuty 보안

Amazon GuardDuty는 AWS 계정 및 워크로드를 지속적으로 모니터링하고 보호할 수 있는 위협 탐지 기능을 제공합니다. Amazon GuardDuty는 이벤트, Amazon VPC 흐름 로그 및 도메인 이름 시스템(DNS) 로그에 AWS CloudTrail 있는 계정 및 네트워크 활동에서 생성된 메타데이터의 연속 스트림을 분석합니다. 또한 알려진 악성 IP 주소, 이상 탐지 및 기계 학습과 같은 통합 위협 인텔리전스를 사용하여 위협을 더 정확하게 식별합니다. GuardDuty는 모니터링되는 AMS 서비스입니다. Amazon GuardDuty 모니터링에 대한 자세한 내용은 섹션을 참조하세요 [GuardDuty 모니터링](#). GuardDuty에 대한 자세한 내용은 [Amazon GuardDuty](#)를 참조하세요.

모든 새 AMS 계정에는 기본적으로 GuardDuty가 활성화되어 있습니다. AMS는 계정 온보딩 중에 GuardDuty를 구성합니다. 언제든지 변경 요청을 제출하여 설정을 수정할 수 있습니다. GuardDuty 요금은 Amazon Elastic Compute Cloud(Amazon EC2)와 같은 다른 서비스와 유사하게 AMS에 적용됩니다. 사용량에 따라 GuardDuty 요금을 지불하고 SLAs에 따라 AMS 증가를 지불합니다. GuardDuty 요금은 Amazon VPC 흐름 로그의 AWS CloudTrail 이벤트 및 볼륨을 기준으로 측정된 사용량([Amazon GuardDuty 요금](#))을 기준으로 합니다.

AMS의 GuardDuty의 경우 다음과 같은 기본 탐지 범주가 활성화됩니다.

- 정찰 -- 비정상적인 API 활동, VPC 내 포트 스캔, 로그인 요청 실패의 비정상적인 패턴 또는 알려진 잘못된 IP에서 검색하는 차단되지 않은 포트와 같은 위협 행위자의 정찰을 제안하는 활동입니다.
- 인스턴스 문제 -- 암호화페 마이닝, 도메인 생성 알고리즘(DGA)을 사용한 맬웨어, 아웃바운드 서비스 활동 거부, 비정상적으로 많은 양의 네트워크 트래픽, 비정상적인 네트워크 프로토콜, 알려진 악성 IP와의 아웃바운드 인스턴스 통신, 외부 IP 주소에서 사용하는 임시 Amazon EC2 자격 증명, DNS를 사용한 데이터 유출과 같은 문제가 있는 인스턴스 활동.
- 계정 활동 - 계정 활동을 나타내는 일반적인 패턴에는 비정상적인 지리적 위치 또는 익명화 프록시의 API 호출, 로깅 비활성화 AWS CloudTrail 시도, 비정상적인 인스턴스 또는 인프라 시작, 비정상적인 AWS 리전의 인프라 배포, 알려진 악성 IP 주소의 API 호출이 포함됩니다.

AMS는 관리형 계정에서 GuardDuty를 사용하여 GuardDuty의 조사 결과 및 알림을 지속적으로 모니터링하고, 알림이 표시되면 AMS 작업은 사전 조치를 취하여 리소스와 계정을 보호합니다. AWS 콘솔 또는 지원되는 통합에서 GuardDuty 조사 결과 및 작업을 펼칠 때 이를 볼 수 있습니다.

GuardDuty는 계정의 Trend Micro Deep Security Manager와 함께 작동합니다. Trend Micro Deep Security Manager는 호스트 기반 침입 탐지/침입 방지 서비스를 제공합니다. Trend Micro Web Reputation 서비스는 호스트가 위협으로 알려진 호스트 또는 웹 서비스와 통신을 시도하는 시기를 감

지하는 기능에서 GuardDuty와 일부 중복됩니다. 그러나 GuardDuty는 추가 위협 탐지 범주를 제공하고 Trend Micro의 호스트 기반 탐지를 보완하는 방법인 네트워크 트래픽을 모니터링하여 이를 달성합니다. 네트워크 기반 위협 탐지를 사용하면 호스트에 문제가 있는 동작이 있는 경우 제어가 실패하지 않도록 하여 보안을 강화할 수 있습니다. AMS는 모든 AMS 계정에서 GuardDuty를 사용할 것을 권장합니다.

Trend Micro에 대해 자세히 알아보려면 [Trend Micro Deep Security Help Center](#)를 참조하세요. Amazon 이외의 링크는 예고 없이 변경될 수 있습니다.

GuardDuty 모니터링

GuardDuty는 AMS가 캡처하고 경고할 수 있는 [보안 조사 결과를](#) 생성하여 AWS 환경의 상태를 알려줍니다.

Amazon GuardDuty는 VPC 흐름 로그, AWS CloudTrail 이벤트 로그 및 도메인 이름 시스템 로그를 분석하고 처리하여 AWS 환경의 보안을 모니터링합니다. 신뢰할 수 있는 사용자 지정 IP 목록 및 위협 목록도 사용하도록 GuardDuty를 구성하여이 모니터링 범위를 확장할 수 있습니다.

- 신뢰할 수 있는 IP 목록은 AWS 인프라 및 애플리케이션과의 보안 통신을 위해 허용한 IP 주소로 구성됩니다. GuardDuty는 신뢰할 수 있는 IP 목록의 IP 주소에 대한 결과를 생성하지 않습니다. 해당 시점에 리전별로 AWS 계정당 신뢰할 수 있는 IP 목록을 하나만 업로드할 수 있습니다.
- 위협 목록은 알려진 악성 IP 주소로 구성되어 있습니다. GuardDuty는 위협 목록을 기반으로 조사 결과를 생성합니다. 해당 시점에 리전별로 AWS 계정당 위협 목록을 최대 6개까지 업로드할 수 있습니다.

GuardDuty를 구현하려면 AMS CT 배포 | 모니터링 및 알림 | GuardDuty IP 세트 | 생성(ct-08avsj2e9mc7g)을 사용하여 승인된 IP 주소 세트를 생성합니다. AMS CT 배포 | 모니터링 및 알림 | GuardDuty 위협 인텔리전스 세트 | 생성(ct-25v6r7t8gvkq5)을 사용하여 거부된 IP 주소 세트를 생성할 수도 있습니다.

AMS가 모니터링하는 서비스 목록은 섹션을 참조하세요 [AMS 모니터링 시스템은 무엇을 모니터링합니까?](#).

Amazon Route 53 Resolver DNS 방화벽

Amazon Route 53 Resolver는 퍼블릭 레코드, Amazon VPC별 DNS 이름 및 Amazon Route 53 프라이빗 호스팅 영역에 대한 AWS 리소스의 DNS 쿼리에 재귀적으로 응답하며 기본적으로 모든 VPCs. Route 53 Resolver DNS 방화벽을 사용하면 Virtual Private Cloud(VPC)에 대한 아웃바운드 DNS 트래픽을 필터링하고 제어할 수 있습니다. 이렇게 하려면 DNS 방화벽 규칙 그룹에 재사용 가능한 필터링

규칙 컬렉션을 생성하고 규칙 그룹을 VPC에 연결한 다음 DNS 방화벽 로그 및 지표 활동을 모니터링합니다. 활동에 따라 DNS 방화벽의 동작을 적절하게 조정할 수 있습니다. 자세한 내용은 [DNS 방화벽을 사용하여 아웃바운드 DNS 트래픽 필터링](#)을 참조하세요.

Route 53 Resolver DNS 방화벽 구성을 보고 관리하려면 다음 절차를 사용합니다.

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/vpc/> Amazon VPC 콘솔을 엽니다.
2. DNS 방화벽에서 규칙 그룹을 선택합니다.
3. 기존 구성을 검토, 편집 또는 삭제하거나 새 규칙 그룹을 생성합니다. 자세한 내용은 [Route 53 Resolver DNS 방화벽 작동 방식](#)을 참조하세요.

Amazon Route 53 Resolver DNS 방화벽 모니터링 및 보안

Amazon Route 53 DNS 방화벽은 규칙 연결, 규칙 작업 및 규칙 평가 우선 순위의 개념을 사용합니다. 도메인 목록(domain list)은 규칙 그룹 내부의 DNS 방화벽 규칙에서 사용하는 재사용 가능한 도메인 사양 집합입니다. 규칙 그룹을 VPC 와 연결하면 DNS 방화벽은 규칙에 사용되는 도메인 목록과 DNS 쿼리를 비교합니다. DNS 방화벽이 일치하는 항목을 찾으면 일치하는 규칙의 작업에 따라 DNS 쿼리를 처리합니다. 규칙 그룹 및 규칙에 대한 자세한 내용은 [DNS 방화벽 규칙 그룹 및 규칙](#)을 참조하세요.

도메인 목록은 두 가지 주요 범주로 나뉩니다.

- 가 자동으로 AWS 생성하고 유지 관리하는 관리형 도메인 목록입니다.
- 생성 및 유지 관리하는 자체 도메인 목록입니다.

규칙 그룹은 연결 우선 순위 인덱스를 기반으로 평가됩니다.

기본적으로 AMS는 다음 규칙과 규칙 그룹으로 구성된 기존 구성을 배포합니다.

- 라는 규칙 그룹 1개DefaultSecurityMonitoringRule. 규칙 그룹은 활성화된 각의 각 기존 VPC에 대해 생성 시 사용할 수 있는 연결 우선 순위가 가장 높습니다 AWS 리전.
- 작업 ALERTDefaultSecurityMonitoringRule와 함께 AWSManagedDomainsAggregateThreatList 관리형 도메인 목록을 사용하여 규칙 그룹 내에서 우선순위가 1인 라는 하나의 DefaultSecurityMonitoringRule 규칙.

기존 구성이 있는 경우 기존 구성보다 우선 순위가 낮은 기존 구성이 배포됩니다. 기존 구성이 기본값입니다. 기존 구성이 쿼리 해결을 처리하는 방법에 대한 우선 순위가 더 높은 지침을 제공하지 않는 경

우 AMS 기준 구성을 catch-all로 사용합니다. 기존 구성을 변경하거나 제거하려면 다음 중 하나를 수행합니다.

- Cloud Service Delivery Manager(CSDM) 또는 Cloud Architect(CA)에 문의하십시오.
- [관리 | 기타 | 기타 | CT 생성\(ct-1e1xtak34nx76\)을 사용하여 변경 요청\(RFC\)을 생성합니다.](#)
- 서비스 요청을 생성하십시오.

계정이 개발자 모드 또는 직접 변경 모드에서 운영되는 경우 직접 변경을 수행할 수 있습니다.

AWS Certificate Manager (ACM) 인증서

AMS에는 CT, 배포 | 고급 스택 구성 요소 | 추가 SANs 포함된 ACM 인증서 | 생성(ct-3l14e139i5p50)이 있으며, 이를 사용하여 최대 5개의 추가 주체 대체 이름(SAN)(예: example.com, example.net, example.org)으로 AWS Certificate Manager 인증서에 대한 요청을 제출할 수 있습니다. 자세한 내용은 [What Is AWS Certificate Manager?](#) 및 [ACM Certificate Characteristic](#)을 참조하세요.

Note

이 제한 시간 설정은 실행뿐만 아니라 이메일 검증을 통한 ACM 인증서 검증에 관한 것입니다. 검증이 없으면 RFC가 실패합니다.

AMS의 데이터 암호화

AMS는 데이터 암호화에 여러 AWS 서비스, 특히 Amazon Simple Storage Service, AWS Key Management Service (AWS KMS), Amazon Elastic Block Store, Amazon Relational Database Service, Amazon Redshift Amazon ElastiCache, AWS Lambda 및 Amazon OpenSearch Service를 사용합니다.

Amazon S3

Amazon S3은 전송 중인 데이터와 유틸리티 시 데이터를 보호하는 몇 가지 객체 암호화 옵션을 제공합니다. 서버 측 암호화는 데이터 센터의 디스크에 저장하기 전에 객체를 암호화하고 객체를 다운로드할 때 암호를 해독합니다. 요청을 인증하기만 하면 액세스 권한을 갖게 되며, 객체의 암호화 여부와 관계없이 액세스 방식에는 차이가 없습니다. 자세한 내용은 [Amazon S3의 데이터 보호](#)를 참조하세요.

Amazon EBS

Amazon EBS 암호화를 사용하면 자체 키 관리 인프라를 구축, 유지 관리 및 보호할 필요가 없습니다. Amazon EBS 암호화는 암호화된 볼륨 및 스냅샷을 생성할 때 AWS KMS 키를 사용합니다. 암호화 작업은 Amazon EC2 인스턴스를 호스팅하는 서버에서 발생합니다. 이는 인스턴스와 연결된 Amazon EBS 스토리지 간에 data-at-rest data-in-transit 모두 안전한지 확인하기 위해 수행됩니다. 인스턴스에는 암호화된 볼륨과 암호화되지 않은 볼륨을 동시에 연결할 수 있습니다. 자세한 내용은 [Amazon EBS 암호화](#)를 참조하세요.

Amazon RDS

Amazon RDS는 Amazon RDS DB 인스턴스를 암호화할 수 있습니다. 저장 시 암호화된 데이터에는 DB 인스턴스의 기본 스토리지, 자동 백업, 읽기 전용 복제본 및 스냅샷이 포함됩니다. Amazon RDS 암호화 DB 인스턴스는 업계 표준 AES-256 암호화 알고리즘을 사용하여 Amazon RDS DB 인스턴스를 호스팅하는 서버의 데이터를 암호화합니다. 데이터가 암호화되면 Amazon RDS는 성능에 최소한의 영향을 미치면서 투명하게 데이터 액세스 인증 및 암호 해독을 처리합니다. 암호화를 사용하도록 데이터베이스 클라이언트 애플리케이션을 수정하지 않아도 됩니다. 자세한 내용은 [Amazon RDS 리소스 암호화](#) 단원을 참조하십시오.

Amazon Simple Queue Service

기본 Amazon SQS 관리형 서버 측 암호화(SSE) 옵션 외에도 Amazon SQS 관리형 SSE(SSE-SQS)를 사용하면 Amazon SQS 관리형 암호화 키를 사용하여 메시지 대기열을 통해 전송되는 민감한 데이터를 보호하는 사용자 지정 관리형 서버 측 암호화를 생성할 수 있습니다. 서버 측 암호화(SSE)를 사용하면 암호화된 대기열에서 민감한 데이터를 전송할 수 있습니다. SSE는 Amazon SQS 관리형 암호화 키(SSE-SQS) 또는 (SSE- AWS KMS KMS)에서 관리되는 키를 사용하여 대기열의 메시지 콘텐츠를 보호합니다. 를 사용하여 SSE를 관리하는 방법에 대한 자세한 내용은 [저장 시 암호화](#)를 AWS Management Console참조하세요.

유휴 시(저장된) 데이터 암호화

OpenSearch Service 도메인은 저장된 데이터 암호화, 데이터 무단 액세스를 방지하는 보안 기능을 제공합니다. 이 기능은 AWS Key Management Service (AWS KMS)를 사용하여 암호화 키를 저장하고 관리하며 고급 암호화 표준 알고리즘을 256비트 키(AES-256)와 함께 사용하여 암호화를 수행합니다. 자세한 내용은 [Amazon OpenSearch Service의 저장 데이터 암호화를 참조하세요](#).

키 관리

AWS KMS 는 데이터를 암호화하는 데 사용되는 암호화 키인 고객 마스터 키(CMKs)를 쉽게 생성하고 제어할 수 있는 관리형 서비스입니다. AWS KMS CMKs는 중국(베이징) 및 중국(닝샤) 리전을 제외하고 FIPS 140-2 암호화 모듈 검증 프로그램에서 검증한 하드웨어 보안 모듈(HSMs)로 보호됩니다. 자세한 내용은 [AWS Key Management Service란?](#)을 참조하십시오.

자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM)는 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 웹 서비스입니다. IAM을 사용하여 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 있음)된 대상을 제어합니다. AMS 온보딩 중에 각 관리형 계정 내에서 교차 계정 IAM 관리자 역할을 생성할 책임은 사용자에게 있습니다.

다중 계정 랜딩 존(MALZ) IAM 보호

AMS 다중 계정 랜딩 존(MALZ)은 각 조직(AMS 및 고객 모두)이 자신의 자격 증명 수명 주기를 관리할 수 있도록 AMS 액세스 관리의 기본 설계 목표로 Active Directory(AD) 신뢰가 필요합니다. 이렇게 하면 서로의 디렉터리에 자격 증명이 필요하지 않습니다. 단방향 신뢰는의 관리형 Active Directory가 고객 소유 또는 관리형 AD를 AWS 계정 신뢰하여 사용자를 인증하도록 구성됩니다. 신뢰는 한 가지 방법일 뿐이므로 고객 Active Directory에서 관리형 AD를 신뢰한다는 의미는 아닙니다.

이 구성에서는 사용자 ID를 관리하는 고객 디렉터리를 사용자 포리스트라고 하며 Amazon EC2 인스턴스가 연결된 관리형 AD를 리소스 포리스트라고 합니다. Windows 인증을 위해 일반적으로 사용되는 Microsoft 설계 패턴입니다. 자세한 내용은 [포리스트 설계 모델을 참조하세요](#).

이 모델을 사용하면 두 조직 모두 해당 수명 주기를 자동화할 수 있으며, 직원이 조직을 떠날 경우 AMS와 사용자 모두 액세스를 신속하게 취소할 수 있습니다. 이 모델이 없으면 두 조직이 공통 디렉터리를 사용한 경우(또는 서로의 디렉터리에서 사용자/그룹을 생성한 경우) 두 조직 모두 시작 및 나가는 직원을 고려하기 위해 추가 워크플로와 사용자 동기화를 적용해야 합니다. 이로 인해 해당 프로세스에 지연 시간이 있고 오류가 발생하기 쉬운 위험이 발생합니다.

MALZ 액세스 사전 조건

AWS/AMS 콘솔, CLI, SDK에 액세스하기 위한 MALZ 자격 증명 공급자 통합.

AMS 계정의 Amazon EC2 인스턴스에 대한 단방향 신뢰.

ID를 통한 인증

AMS는 IAM 자격 증명의 한 유형인 IAM 역할을 사용합니다. IAM 역할은에서 자격 증명이 수행할 수 있는 작업과 수행할 수 없는 작업을 결정하는 권한 정책이 있는 자격 증명이라는 점에서 사용자와 매우 유사합니다 AWS. 그러나 역할에는 자격 증명이 연결되어 있지 않으므로 한 사람과 고유하게 연결되는 대신 역할이 필요한 모든 사용자가 역할을 수입할 수 있습니다. IAM 사용자는 한 가지 역할을 맡음으로써 특정 작업을 위해 다른 권한을 임시로 얻을 수 있습니다.

액세스 역할은 Operations Management에서 관리하고 정기적으로 검토하는 내부 그룹 멤버십에 의해 제어됩니다.

AMS의 IAM 사용자 역할

IAM 역할은 자격 AWS 증명이 할 수 있는 것과 없는 것을 결정하는 권한 정책이 있는 자격 증명이라는 점에서 IAM 사용자와 유사합니다 AWS. 그러나 역할은 한 사람하고만 연관되지 않고 해당 역할이 필요한 사람이라면 누구든지 맡을 수 있어야 합니다.

현재 Customer_ReadOnly_Role표준 AMS 계정의 경우 AMS 기본 사용자 역할 1개가 있고 관리형 Active Directory가 있는 AMS 계정customer_managed_ad_user_role의 경우 추가 역할 1개가 있습니다.

역할 정책은 CloudWatch 및 Amazon S3 로그 작업, AMS 콘솔 액세스, 대부분의 읽기 전용 제한, 계정 S3 콘솔에 대한 AWS 서비스제한된 액세스, AMS 변경 유형 액세스에 대한 권한을 설정합니다.

또한 Customer_ReadOnly_Role에는 인스턴스를 예약할 수 있는 변경 가능한 예약 인스턴스 권한이 있습니다. 일부 비용 절감 값이 있으므로 특정 수의 Amazon EC2 인스턴스가 장기간 필요할 경우 해당 APIs. 자세한 내용은 [Amazon EC2 예약 인스턴스를 참조하세요](#).

Note

기존 정책을 재사용하지 않는 한, IAM 사용자에게 대한 사용자 지정 IAM 정책을 생성하기 위한 AMS 서비스 수준 목표(SLO)는 영업일 기준 4일입니다. 기존 IAM 사용자 역할을 수정하거나 새 역할을 추가하려면 각각 [IAM: 개체 업데이트](#) 또는 [IAM: 개체 RFC 생성](#)을 제출합니다.

Amazon IAM 역할에 익숙하지 않은 경우 [IAM 역할에서 중요한 정보를 참조하세요](#).

다중 계정 랜딩 존(MALZ): AMS 다중 계정 랜딩 존의 사용자 지정되지 않은 기본 사용자 역할 정책을 보려면 다음 단원[MALZ: 기본 IAM 사용자 역할](#)을 참조하십시오.

MALZ: 기본 IAM 사용자 역할

기본 다중 계정 AMS 다중 계정 랜딩 존 사용자 역할에 대한 JSON 정책 설명입니다.

Note

사용자 역할은 사용자 지정할 수 있으며 계정별로 다를 수 있습니다. 역할을 찾는 방법에 대한 지침이 제공됩니다.

다음은 기본 MALZ 사용자 역할의 예입니다. 필요한 정책이 설정되어 있는지 확인하려면 AWS 명령을 실행 [get-role](#)하거나 AWS 관리 -> [IAM 콘솔](#)에 로그인하고 탐색 창에서 역할을 선택합니다.

코어 OU 계정 역할

코어 계정은 MALZ 관리형 인프라 계정입니다. AMS 다중 계정 랜딩 존 코어 계정에는 관리 계정과 네트워킹 계정이 포함됩니다.

코어 OU 계정: 공통 역할 및 정책

역할	정책 또는 정책
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (퍼블릭 AWS 관리형 정책).
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportAccess (퍼블릭 AWS 관리형 정책).
AWSManagedServicesChangeManagementRole(코어 계정 버전)	ReadOnlyAccess AWSSupportAccess AMSChangeManagementReadOnlyPolicy AMSChangeManagementInfrastructurePolicy

코어 OU 계정: 관리 계정 역할 및 정책

역할	정책 또는 정책
AWSManagedServicesBillingRole	AMSBillingPolicy (AMSBillingPolicy).
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (퍼블릭 AWS 관리형 정책).
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportAccess (퍼블릭 AWS 관리형 정책).
AWSManagedServicesChangeManagementRole(관리 계정 버전)	ReadOnlyAccess AWSSupportAccess

역할	정책 또는 정책
	AMSCChangeManagementReadOnlyPolicy
	AMSCChangeManagementInfrastructurePolicy
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

코어 OU 계정: 네트워킹 계정 역할 및 정책

역할	정책 또는 정책
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (퍼블릭 AWS 관리형 정책).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess (퍼블릭 AWS 관리형 정책).
AWSManagedServicesChangeManagementRole(네트워킹 계정 버전)	ReadOnlyAccess
	AWSSupportAccess
	AMSCChangeManagementReadOnlyPolicy
	AMSCChangeManagementInfrastructurePolicy
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

애플리케이션 계정 역할

애플리케이션 계정 역할은 애플리케이션별 계정에 적용됩니다.

애플리케이션 계정: 역할 및 정책

역할	정책 또는 정책
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (퍼블릭 AWS 관리형 정책).

역할	정책 또는 정책
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupportAccess(퍼블릭 AWS 관리형 정책). 이 정책은 모든 지원 작업 및 리소스에 대한 액세스를 제공합니다. 자세한 내용은 AWS Support 시작하기를 참조하세요.
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess AWSSupportAccess 예제 이 정책은 모든 지원 작업 및 리소스에 대한 액세스를 제공합니다. AWSCertificateManagerFullAccess 정보, (퍼블릭 AWS 관리형 정책) AWSWAFFullAccess information, (퍼블릭 AWS 관리형 정책). 이 정책은 AWS WAF 리소스에 대한 전체 액세스 권한을 부여합니다. AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole(애플리케이션 계정 버전)	ReadOnlyAccess AWSSupportAccess(퍼블릭 AWS 관리형 정책). 이 정책은 모든 지원 작업 및 리소스에 대한 액세스를 제공합니다. 자세한 내용은 AWS Support 시작하기를 참조하세요. AMSSecretsManagerSharedPolicy AMSChangeManagementPolicy AMSReservedInstancesPolicy AMSS3Policy

역할	정책 또는 정책
AWSManagedServicesAdminRole	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAccess
	AMSS3Policy
	AMSReservedInstancesPolicy

정책 예제

사용되는 대부분의 정책에 대한 예제가 제공됩니다. 활성 AWS 계정이 있는 경우 [ReadOnlyAccess](#) 정책(모든 AWS 서비스에 대한 읽기 전용 액세스를 제공하는 페이지)을 보려면이 링크를 사용할 수 [ReadOnlyAccess](#). 또한 요약된 버전이 여기에 포함되어 있습니다.

AMSBillingPolicy

AMSBillingPolicy

회계 부서에서 새 결제 역할을 사용하여 관리 계정의 결제 정보 또는 계정 설정을 보고 변경할 수 있습니다. 대체 연락처와 같은 정보에 액세스하거나, 계정 리소스 사용량을 보거나, 결제 탭을 유지하거나, 결제 방법을 수정하려면이 역할을 사용합니다. 이 새 역할은 [AWS Billing IAM 작업 웹 페이지에](#) 나열된 모든 권한으로 구성됩니다.

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Action": [
      "aws-portal:ViewBilling",
      "aws-portal:ModifyBilling"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToBilling"
  },
  {
    "Action": [
      "aws-portal:ViewAccount",
      "aws-portal:ModifyAccount"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToAccountSettings"
  },
  {
    "Action": [
      "budgets:ViewBudget",
      "budgets:ModifyBudget"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToAccountBudget"
  },
  {
    "Action": [
      "aws-portal:ViewPaymentMethods",
      "aws-portal:ModifyPaymentMethods"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToPaymentMethods"
  },
  {
    "Action": [
      "aws-portal:ViewUsage"
    ],
    "Resource": "*",
    "Effect": "Allow",
```

```

        "Sid": "AllowAccessToUsage"
    },
    {
        "Action": [
            "cur:DescribeReportDefinitions",
            "cur:PutReportDefinition",
            "cur>DeleteReportDefinition",
            "cur:ModifyReportDefinition"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AllowAccessToCostAndUsageReport"
    },
    {
        "Action": [
            "pricing:DescribeServices",
            "pricing:GetAttributeValues",
            "pricing:GetProducts"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AllowAccessToPricing"
    },
    {
        "Action": [
            "ce:*",
            "compute-optimizer:*"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AllowAccessToCostExplorerComputeOptimizer"
    },
    {
        "Action": [
            "purchase-orders:ViewPurchaseOrders",
            "purchase-orders:ModifyPurchaseOrders"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AllowAccessToPurchaseOrders"
    },
    {
        "Action": [
            "redshift:AcceptReservedNodeExchange",

```

```

        "redshift:PurchaseReservedNodeOffering"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToRedshiftAction"
  },
  {
    "Action": "savingsplans:*",
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AWSSavingsPlansFullAccess"
  }
]
}

```

AMSChangeManagementReadOnlyPolicy

AMSChangeManagementReadOnlyPolicy

모든 AMS 변경 유형과 요청된 변경 유형의 기록을 볼 수 있는 권한.

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

배포 | 관리형 랜딩 존 | 관리 계정 | 애플리케이션 계정 생성(VPC 사용) 변경 유형을 요청할 수 있는 권한.

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

배포 | 관리형 랜딩 존 | 네트워킹 계정 | 애플리케이션 라우팅 테이블 변경 유형 생성을 요청할 수 있는 권한.

AMSChangeManagementInfrastructurePolicy

AMSChangeManagementInfrastructurePolicy (관리용 | 기타 | 기타 CTs)

관리 | 기타 | 기타 | 생성 및 관리 | 기타 | 기타 | 변경 유형 업데이트를 요청할 수 있는 권한.

AMSSecretsManagerSharedPolicy

AMSSecretsManagerSharedPolicy

를 통해 AMS에서 공유하는 보안 암호/해시를 볼 수 있는 권한 AWS Secrets Manager (예: 감사를 위한 인프라에 대한 암호).

AMS와 공유할 보안 암호/해시를 생성할 수 있는 권한(예: 배포해야 하는 제품의 라이선스 키).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowAccessToSharedNameSpaces",
    "Effect": "Allow",
    "Action": "secretsmanager:*",
    "Resource": [
      "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
      "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    ]
  },
  {
    "Sid": "DenyGetSecretOnCustomerNamespace",
    "Effect": "Deny",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
    "Sid": "AllowReadAccessToAMSNameSpace",
    "Effect": "Deny",
    "NotAction": [
      "secretsmanager:Describe*",
      "secretsmanager:Get*",
      "secretsmanager:List*"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
  ]
}
```

AMSChangeManagementPolicy

AMSChangeManagementPolicy

모든 AMS 변경 유형 및 요청된 변경 유형의 기록을 요청하고 볼 수 있는 권한.

AMSReservedInstancesPolicy

AMSReservedInstancesPolicy

Amazon EC2 예약 인스턴스를 관리할 수 있는 권한. 요금 정보는 [Amazon EC2 예약 인스턴스를 참조하세요](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowReservedInstancesManagement",
    "Effect": "Allow",
    "Action": [
      "ec2:ModifyReservedInstances",
      "ec2:PurchaseReservedInstancesOffering"
    ],
    "Resource": [
      "*"
    ]
  }]
}
```

AMSS3Policy

AMSS3Policy

기존 Amazon S3 버킷에서 파일을 생성하고 삭제할 수 있는 권한.

Note

이러한 권한은 배포 | 고급 스택 구성 요소 | S3 스토리지 | 변경 유형 생성으로 수행해야 하는 S3 버킷을 생성할 수 있는 권한을 부여하지 않습니다.

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:AbortMultipartUpload",
      "s3:DeleteObject",
      "s3:PutObject"
    ],
    "Resource": "*"
  }
]
```

AWSSupportAccess

AWSSupportAccess

에 대한 전체 액세스 권한 지원. 자세한 내용은 [시작하기를 참조하세요 지원](#). Premium Support에 대한 자세한 내용은 섹션을 참조하세요 [지원](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "support:*"
    ],
    "Resource": "*"
  }]
}
```

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions (공개 AWS관리형 정책)

구독, 구독 취소 및 AWS Marketplace 구독 보기 권한.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "aws-marketplace:ViewSubscriptions",
      "aws-marketplace:Subscribe",
      "aws-marketplace:Unsubscribe"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess

에 대한 전체 액세스 권한 AWS Certificate Manager. 자세한 내용은 [AWS Certificate Manager](#) 단원을 참조하십시오.

[AWSCertificateManagerFullAccess](#) information, (퍼블릭 AWS 관리형 정책).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "acm:*"
    ],
    "Resource": "*"
  }]
}
```

AWSWAFFullAccess

AWSWAFFullAccess

에 대한 전체 액세스 권한 AWS WAF. 자세한 내용은 [AWS WAF - 웹 애플리케이션 방화벽](#)을 참조하세요.

[AWSWAFFullAccess](#) information, (퍼블릭 AWS 관리형 정책). 이 정책은 AWS WAF 리소스에 대한 전체 액세스 권한을 부여합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "waf:*",
      "waf-regional:*",
      "elasticloadbalancing:SetWebACL"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

ReadOnlyAccess

ReadOnlyAccess

AWS 콘솔의 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스. 가 새 서비스를 AWS 시작하면 AMS는 ReadOnlyAccess 정책을 업데이트하여 새 서비스에 대한 읽기 전용 권한을 추가합니다. 이렇게 업데이트된 권한은 정책이 추가되는 모든 보안 주체 엔터티에게 적용됩니다.

이렇게 해도 EC2 호스트 또는 데이터베이스 호스트에 로그인할 수 있는 기능은 부여되지 않습니다.

활성이 있는 경우이 링크 [ReadOnlyAccess](#)를 사용하여 전체 ReadOnlyAccess 정책을 볼 AWS 계정 수 있습니다. 전체 ReadOnlyAccess 정책은 모든에 대한 읽기 전용 액세스를 제공하는 한 매우 깁니다 AWS 서비스. 다음은 ReadOnlyAccess 정책의 부분 발췌문입니다.

단일 계정 랜딩 존(SALZ): AMS 단일 계정 랜딩 존 기본 사용자 지정되지 않은 사용자 역할 정책을 보려면 [SALZ: 기본 IAM 사용자 역할](#)다음을 참조하세요.

SALZ: 기본 IAM 사용자 역할

기본 AMS 단일 계정 랜딩 존 사용자 역할에 대한 JSON 정책 설명입니다.

Note

SALZ 기본 사용자 역할은 사용자 지정할 수 있으며 계정별로 다를 수 있습니다. 역할을 찾는 방법에 대한 지침이 제공됩니다.

다음은 기본 SALZ 사용자 역할의 예입니다. 정책이 설정되어 있는지 확인하려면 [get-role](#) 명령을 실행합니다. 또는 <https://console.aws.amazon.com/iam/> AWS Identity and Access Management 콘솔에 로그인한 다음 역할을 선택합니다.

고객 읽기 전용 역할은 여러 정책의 조합입니다. 역할 분석(JSON)은 다음과 같습니다.

관리형 서비스 감사 정책:

관리형 서비스 IAM ReadOnly 정책

관리형 서비스 사용자 정책

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomerToListTheLogBucketLogs",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "aws/*",
            "app/*",
            "encrypted",
            "encrypted/",
            "encrypted/app/*"
          ]
        }
      }
    }
  ],
}
```

```
{
  "Sid": "BasicAccessRequiredByS3Console",
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": [
    "arn:aws:s3:::*"
  ]
},
{
  "Sid": "AllowCustomerToGetLogs",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject*"
  ],
  "Resource": [
    "arn:aws:s3:::mc-a*-logs-*/aws/*",
    "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
  ]
},
{
  "Sid": "AllowAccessToOtherObjects",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteObject*",
    "s3:Get*",
    "s3:List*",
    "s3:PutObject*"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "AllowCustomerToListTheLogBucketRoot",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::mc-a*-logs-*"
  ]
},
```

```
    "Condition": {
      "StringEquals": {
        "s3:prefix": [
          "",
          "/"
        ]
      }
    }
  },
  {
    "Sid": "AllowCustomerCWLConsole",
    "Effect": "Allow",
    "Action": [
      "logs:DescribeLogStreams",
      "logs:DescribeLogGroups"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:*"
    ]
  },
  {
    "Sid": "AllowCustomerCWLAccessLogs",
    "Effect": "Allow",
    "Action": [
      "logs:FilterLogEvents",
      "logs:GetLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/*",
      "arn:aws:logs:*:*:log-group:/infra/*",
      "arn:aws:logs:*:*:log-group:/app/*",
      "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
    ]
  },
  {
    "Sid": "AWSManagedServicesFullAccess",
    "Effect": "Allow",
    "Action": [
      "amscm:*",
      "amsskms:*"
    ],
    "Resource": [
      "*"
    ]
  }
]
```

```
},
{
  "Sid": "ModifyAWSBillingPortal",
  "Effect": "Allow",
  "Action": [
    "aws-portal:Modify*"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "DenyDeleteCWL",
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:*"
  ]
},
{
  "Sid": "DenyMCCWL",
  "Effect": "Deny",
  "Action": [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DescribeLogStreams",
    "logs:FilterLogEvents",
    "logs:GetLogEvents",
    "logs:PutLogEvents"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:/mc/*"
  ]
},
{
  "Sid": "DenyS3MCNamespace",
  "Effect": "Deny",
  "Action": [
    "s3:*"
  ],
  "Resource": [
```

```

        "arn:aws:s3::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3::mc-a*-logs-*/mc/*",
        "arn:aws:s3::mc-a*-logs-*audit/*",
        "arn:aws:s3::mc-a*-internal-*/*",
        "arn:aws:s3::mc-a*-internal-*"
    ]
},
{
    "Sid": "ExplicitDenyS3CfnBucket",
    "Effect": "Deny",
    "Action": [
        "s3:*"
    ],
    "Resource": [
        "arn:aws:s3::cf-templates-*"
    ]
},
{
    "Sid": "DenyListBucketS3LogsMC",
    "Action": [
        "s3:ListBucket"
    ],
    "Effect": "Deny",
    "Resource": [
        "arn:aws:s3::mc-a*-logs-*"
    ],
    "Condition": {
        "StringLike": {
            "s3:prefix": [
                "auditlog/*",
                "encrypted/mc/*",
                "mc/*"
            ]
        }
    }
},
{
    "Sid": "DenyS3LogsDelete",
    "Effect": "Deny",
    "Action": [
        "s3:Delete*",
        "s3:Put*"
    ],
    "Resource": [

```

```
    "arn:aws:s3:::mc-a*-logs-*/*"
  ],
},
{
  "Sid": "DenyAccessToKmsKeysStartingWithMC",
  "Effect": "Deny",
  "Action": [
    "kms:*"
  ],
  "Resource": [
    "arn:aws:kms::*:key/mc-*",
    "arn:aws:kms::*:alias/mc-*"
  ]
},
{
  "Sid": "DenyListingOfStacksStartingWithMC",
  "Effect": "Deny",
  "Action": [
    "cloudformation:*"
  ],
  "Resource": [
    "arn:aws:cloudformation::*:stack/mc-*"
  ]
},
{
  "Sid": "AllowCreateCWMetricsAndManageDashboards",
  "Effect": "Allow",
  "Action": [
    "cloudwatch:PutMetricData"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "AllowCreateandDeleteCWDashboards",
  "Effect": "Allow",
  "Action": [
    "cloudwatch:DeleteDashboards",
    "cloudwatch:PutDashboard"
  ],
  "Resource": [
    "*"
  ]
}
```



```
}  
]  
}
```

Customer Secrets Manager 공유 정책

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AllowSecretsManagerListSecrets",  
      "Effect": "Allow",  
      "Action": "secretsmanager:listSecrets",  
      "Resource": "*"  
    },  
    {  
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",  
      "Effect": "Allow",  
      "Action": "secretsmanager:*",  
      "Resource": [  
        "arn:aws:secretsmanager:*:secret:ams-shared/*",  
        "arn:aws:secretsmanager:*:secret:customer-shared/*"  
      ]  
    },  
    {  
      "Sid": "DenyCustomerGetSecretCustomerNamespace",  
      "Effect": "Deny",  
      "Action": "secretsmanager:GetSecretValue",  
      "Resource": "arn:aws:secretsmanager:*:secret:customer-shared/*"  
    },  
    {  
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",  
      "Effect": "Deny",  
      "NotAction": [  
        "secretsmanager:Describe*",  
        "secretsmanager:Get*",  
        "secretsmanager:List*"  
      ],  
      "Resource": "arn:aws:secretsmanager:*:secret:ams-shared/*"  
    }  
  ]  
}
```

```
}
```

Customer Marketplace 구독 정책

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

보안 이벤트 로깅 및 모니터링

AMS는 관리형 환경에서 보안 위협을 지속적으로 모니터링합니다. 보안 이벤트는 AMS 또는 사용자가 감지할 수 있습니다. AMS는 미국 국립표준기술연구소(NIST)의 컴퓨터 보안 인시던트 처리 가이드에 따라 자동화 프로세스를 정기적으로 업데이트하여 보안 위협을 더 잘 탐지합니다.

엔드포인트 보안(EPS)

AMS Advanced 환경에서 프로비저닝하는 리소스에는 엔드포인트 보안(EPS) 모니터링 클라이언트 설치가 자동으로 포함됩니다. 이 프로세스를 통해 AMS Advanced 관리형 리소스를 모니터링하고 연중무휴로 지원할 수 있습니다. 또한 AMS Advanced는 모든 에이전트 활동을 모니터링하고 보안 이벤트가 감지되면 인시던트가 생성됩니다.

Note

보안 인시던트는 인시던트로 처리됩니다. 자세한 내용은 [인시던트 대응](#)을 참조하세요.

엔드포인트 보안은 맬웨어 방지 보호를 제공합니다. 특히 다음 작업이 지원됩니다.

- EC2 인스턴스가 EPS에 등록
- EPS에서 EC2 인스턴스 등록 취소
- EC2 인스턴스 실시간 맬웨어 방지 보호
- EPS 에이전트 시작 하트비트
- 격리된 파일 EPS 복원
- EPS 이벤트 알림
- EPS 보고

AMS Advanced는 엔드포인트 보안(EPS)에 Trend Micro를 사용합니다. 이는 기본 EPS 설정입니다. Trend Micro에 대해 자세히 알아보려면 [Trend Micro Deep Security Help Center](#)를 참조하세요. Amazon 이외의 링크는 예고 없이 변경될 수 있습니다.

AMS 고급 다중 계정 랜딩 존(MALZ) 기본 설정은 다음 섹션에 설명되어 있습니다. 기본이 아닌 AMS 다중 계정 랜딩 존 EPS 설정은 [AMS 고급 다중 계정 랜딩 존 EPS 기본이 아닌 설정](#)을 참조하세요.

Note

자체 EPS를 가져올 수 있습니다. [AMS 자체 EPS 가져오기](#)를 참조하세요.

일반 EPS 설정

엔드포인트 보안 일반 네트워크 설정.

EPS 기본값

설정	기본값
방화벽 포트(인스턴스의 보안 그룹)	EPS Deep Security Manager 에이전트(DSMs)는 Agent/Relay to Manager 통신을 위해 포트 41200이 열려 있고 Manager 콘솔을 위해 포트

설정	기본값
	4119가 열려 있어야 합니다. 관리자/에이전트에서 릴레이로 통신하려면 EPS 릴레이에 포트 4122가 열려 있어야 합니다. 에이전트가 모든 요청을 시작하기 때문에 고객 인스턴스 인바운드 통신을 위해 특정 포트를 열면 안 됩니다.
통신 방향	에이전트/어플라이언스 시작됨
하트비트 간격	10분
알림 전 누락된 하트비트 수	2
서버 시간 간에 허용되는 최대 드리프트(차이)	무제한
비활성(등록되었지만 온라인이 아닌) 가상 머신에 대한 오프라인 오류 발생	아니요
기본 정책	기본 정책(다음 설명 참조)
호스트 이름이 동일한 여러 컴퓨터 활성화	허용됨
보류 중인 업데이트에 대한 알림이 발생합니다.	7일 후
일정 업데이트	AMS는 Trend Micro Deep Security Manager(DSM)/Deep Security Agent(DSA) 소프트웨어 업데이트를 위한 월간 릴리스 주기를 목표로 합니다. 그러나 AMS는 업데이트를 위해 SLA를 유지 관리하지 않습니다. 업데이트는 배포 중에 AMS 개발자 팀이 플릿 전체에서 수행합니다. DSA/DSA 업데이트는 AMS가 기본적으로 13주 동안 로컬로 보관하는 Trend MicroDSM 시스템 이벤트에 기록됩니다. 공급업체 설명서는 Trend Micro Deep Security Help Center의 시스템 이벤트를 참조하세요. 로그는 Amazon CloudWatch의 로그 그룹 /aws/ams/eps/var/log/DSM.log로 보내집니다.

설정	기본값
소스 업데이트	Trend Micro 업데이트 서버(https://ipv6-ia.us.trendmicro.com/iau_server.dll/)
이벤트 또는 로그 데이터 삭제	이벤트 및 로그는 7일 후에 Amazon 데이터베이스에서 삭제됩니다.
에이전트 소프트웨어 버전이 보류됨	최대 5개
최신 규칙 업데이트가 보류됨	최대 10개
로그 스토리지	기본적으로 로그 파일은 Amazon S3에 안전하게 저장되지만 감사 및 규정 준수 요구 사항을 충족하는 데 도움이 되도록 Amazon Glacier에 보관할 수도 있습니다.

기본 정책

엔드포인트 보안 기본 정책 기본 설정입니다.

EPS 기본 정책

설정	기본값
활성화된 모듈	맬웨어 방지
비활성화된 모듈	웹 평판
	방화벽
	침입 방지
	무결성 모니터링
	로그 검사
	애플리케이션 제어

맬웨어 방지

엔드포인트 보안 맬웨어 방지 설정.

EPS 맬웨어 방지 기본값

설정	기본값	참고
실시간 스캔	모든 항목 스캔 매일/전일(24시간)	의심되는 모든 바이러스를 격리합니다. IntelliTrap 및 스파이웨어/그레이웨어 보호를 활성화합니다. 스�파이웨어 및 그레이웨어는 맬웨어 방지를 트리거하여 항목을 격리합니다.
수동 스캔	모든 항목 스캔	요청해야 하며, 그런 다음 기본 실시간 스캔 구성을 따릅니다.
예약된 스캔	모든 항목 스캔	매월 마지막 일요일 오전 6시로 설정합니다.
스마트 보호	비활성	N/A
격리된 파일	Trend Micro Deep Security Manager(DSM)	격리용으로 예약된 디스크 약 1GB.
스캔 제한	Trend Micro"	모든 크기의 파일을 스캔합니다.
허용된 스파이웨어 또는 그레이웨어	없음	N/A
로컬 이벤트 알림	예	N/A

맬웨어 완화 프로세스

AMS는 Trend Micro의 Deep Security Platform(맬웨어 방지 시스템)을 사용하여 AMS 관리형 인스턴스에서 맬웨어를 탐지하고 이에 대응합니다. 기본적으로 Trend Micro 감지 에이전트는 Windows 및 Linux 운영 체제 모두에 대해 공유 서비스 및 프라이빗 서브넷의 인스턴스를 포함하여 모든 Amazon EC2 인스턴스에서 실행됩니다. 맬웨어 방지 시스템은 AMS 모니터링에 연결되어 맬웨어가 감지될 때마다 이벤트가 생성됩니다. 고객에게 영향을 미치는 경우 이벤트가 인시던트 관리 프로세스로 에스컬레이션됩니다(자세한 내용은 참조 [AMS 인시던트 대응](#)). AMS가 영향을 평가하는 동안 알림을 받고 영향을 완화하기 위한 시도가 이루어집니다.

Trend Micro가 업데이트를 게시하면 Trend Micro 맬웨어 방지 정의가 자동으로 업데이트됩니다.

애플리케이션 온보딩 중에 인스턴스에서 맬웨어가 발견될 때 AMS가 수행할 작업을 지정합니다.

- 격리된 파일이 허용 목록에 있는지 확인하고 격리에서 제거한 다음 파일 시스템으로 다시 릴리스합니다.
- 격리된 파일을 삭제하여 인스턴스에서 제거합니다.
- 인스턴스를 일시 중지하고 교체합니다. 그러면 일시 중지된 인스턴스를 포렌식 연구를 위해 탑재할 수 있습니다.

애플리케이션 온보딩 후:

- 맬웨어 방지 시스템이 인스턴스에서 맬웨어를 발견하면 AMS는 맬웨어를 자동으로 격리합니다. 그러면 이벤트와 후속 조사가 트리거됩니다.
- AMS는 서비스 알림을 통해 이벤트를 알리고 선택한 기본 완화 작업을 따르기 시작합니다.
- 기본 작업을 선택하지 않은 경우 AMS는 수행할 작업을 묻습니다. 지침을 받은 후 AMS는 선택한 작업을 실행하고 사용자에게 알립니다. 해당하는 경우 AMS는 포렌식 분석에 필요한 세부 정보를 포함하여 작업이 완료된 후 다시 알립니다.

Trend Micro Deep Security에서 IDS 및 IPS 활성화

AMS가 계정에 대해 기본이 아닌 기능인 Trend Micro Intrusion Detection System(IDS) 및 Intrusion Protection Systems(IPS)를 활성화하도록 요청할 수 있습니다.

이렇게 하려면 업데이트 요청(관리 | 기타 | 기타 | 업데이트)을 제출하고 IDS 및 IPS 알림을 수신할 이메일 주소 목록을 포함합니다. 이러한 주소는 AMS가 자동으로 생성하는 계정의 SNS 주제에 추가됩니다.

Note

AMS는 다른 AMS 서비스를 제공하는 기능을 방해할 수 있는 Trend Micro 서비스를 추가할 수 없습니다.

전체 시스템 맬웨어 스캔

PCI DSS(Payment Card Industry Data Security Standard)에는 AMS 관리형 VPC에서 기본적으로 활성화되는 전체 시스템 맬웨어 스캔이 필요합니다. 전체 시스템 스캔은 CPU를 많이 사용하기 때문에 2AM시(서버에 설정된 시간대)에 실행되도록 설정됩니다. 전체 시스템 스캔은 CPU를 많이 사용하지 않는 정기적인 맬웨어 스캔에 추가됩니다.

전체 시스템 맬웨어 스캔을 비활성화할 수 있는 새로운 관리 변경 유형(CT)인 맬웨어 스캔 비활성화가 있습니다. CT는 관리 | 호스트 보안 | 전체 시스템 스캔 | 분류 비활성화, ID 변경 ct-1pybwg08h8qsz에서 찾을 수 있습니다. 스캔을 다시 활성화하려면 관리 | 기타 | 기타 | CT 업데이트를 사용합니다. 전체 시스템 스캔을 비활성화해도 일반 맬웨어 스캔은 비활성화되지 않습니다.

Amazon Inspector 보안

Amazon Inspector 서비스는 AMS 관리형 스택의 보안을 모니터링합니다. Amazon Inspector는 배포된 인프라의 보안 및 규정 준수 격차를 식별하는 데 도움이 되는 자동화된 보안 평가 서비스입니다. AWS. Amazon Inspector 보안 평가를 사용하면 Amazon EC2 인스턴스에서 의도하지 않은 네트워크 액세스 가능성 및 취약성을 확인하여 스택의 노출, 취약성 및 모범 사례와의 편차를 자동으로 평가할 수 있습니다. 평가를 수행한 후, Amazon Inspector는 상세한 보안 평가 결과 목록을 제공하며, 이 목록은 심각도 수준에 따라 구성되어 있습니다. Amazon Inspector 평가는 일반적인 보안 모범 사례 및 정의에 매핑된 사전 정의된 규칙 패키지로 제공됩니다. 이러한 규칙은 AWS 보안 연구원이 정기적으로 업데이트합니다. Amazon Inspector에 대한 자세한 내용은 [Amazon Inspector](#)를 참조하십시오.

AMS Amazon Inspector FAQs

- Amazon Inspector는 기본적으로 AMS 계정에 설치되나요?

아니요. Amazon Inspector는 기본 AMI 빌드 또는 워크로드 수집의 일부가 아닙니다.

- Amazon Inspector에 액세스하고 설치하려면 어떻게 해야 하나요?

RFC(관리 | 기타 | 기타 | 생성)를 제출하여 Inspector에 계정 액세스 및 설치를 요청하면 AMS 운영 팀이 Customer_ReadOnly_Role을 수정하여 Amazon Inspector 콘솔 액세스(SSM 액세스 없음)를 제공합니다.

- 평가하려는 모든 Amazon EC2 인스턴스에 Amazon Inspector 에이전트를 설치해야 합니까?
Amazon EC2

아니요. 네트워크 연결성 규칙 패키지가 포함된 Amazon Inspector 평가는 모든 Amazon EC2 인스턴스에 대해 에이전트 없이 실행할 수 있습니다. 호스트 평가 규칙 패키지에는 에이전트가 필요합니다. 에이전트 설치에 대한 자세한 내용은 [Amazon Inspector 에이전트 설치를 참조하세요](#).

- 이 서비스에 대한 추가 비용이 있습니까?

예. Amazon Inspector 요금은 [Amazon Inspector 요금](#) 사이트에서 확인할 수 있습니다.

- Amazon Inspector 조사 결과란 무엇입니까?

결과는 선택한 평가 대상의 Amazon Inspector 평가 중에 발견된 잠재적 보안 문제입니다. 결과는 Amazon Inspector 콘솔 또는 API에 표시되며 보안 문제에 대한 자세한 설명과 문제 해결을 위한 권장 사항을 모두 포함합니다.

- Amazon Inspector 평가 보고서를 사용할 수 있나요?

예. 평가 보고서는 평가 실행에서 테스트한 내용과 평가 결과를 자세히 설명하는 문서입니다. 평가 결과는 표준 보고서로 형식이 지정되며, 이를 생성하여 문제 해결을 위해 팀 내에서 결과를 공유하거나, 규정 준수 감사 데이터를 보강하거나, 향후 참조를 위해 저장할 수 있습니다. 평가 실행이 성공적으로 완료되면 Amazon Inspector 평가 보고서를 생성할 수 있습니다.

- 태그를 사용하여 Amazon Inspector 보고서를 실행할 스택을 식별할 수 있나요?

예.

- AMS 운영 팀은 Amazon Inspector 평가 결과에 액세스할 수 있나요?

예. AWS의 Amazon Inspector 콘솔에 액세스할 수 있는 사람은 누구나 조사 결과 및 평가 보고서를 볼 수 있습니다.

- AMS 운영 팀은 Amazon Inspector 보고서의 조사 결과에 따라 권장하거나 조치를 취합니까?

아니요. Amazon Inspector 보고서의 결과를 기반으로 변경하려는 경우 RFC(관리 | 기타 | 기타 | 업데이트)를 통해 변경을 요청해야 합니다.

- Amazon Inspector 보고서를 실행할 때 AMS에 알림이 제공되나요?

Amazon Inspector 액세스를 요청하면 RFC를 실행하는 AMS 운영자가 CSDM에 요청을 알립니다.

자세한 내용은 [Amazon Inspector FAQs](#).

AMS 인시던트 대응

AMS는 기존 IT 서비스 관리(ITSM) 인시던트 관리 모범 사례를 사용하여 필요한 경우 최대한 빨리 서비스를 복원합니다.

대시보드와 인시던트 대기열follow-the-sun 지원을 제공합니다.

운영 엔지니어는 내부 인시던트 추적 도구를 사용하여 인시던트를 식별, 로그, 분류, 우선 순위 지정, 진단, 해결 및 종료하고 AMS 콘솔 또는 지원 API를 통해 이러한 모든 활동에 대한 업데이트를 제공합니다. 많은 운영자가 다양한 기술 프로필 및 역할의 AWS Premium Support에서 시간을 보냈으며 다양한 내부 지원 도구를 활용하여 이러한 모든 활동을 지원합니다. 이러한 운영자는 AMS 지원 인프라에 대해 깊이 숙지하고 식별된 모든 지원 문제를 해결할 수 있는 전문가 수준의 기술 역량을 갖추고 있습니다. 드물게 운영자에게 지원이 필요한 경우 Premium Support 및 AWS 서비스 팀이 필요에 따라 지원할 수 있습니다.

우선순위가 높은 인시던트가 중요한 워크로드에 영향을 미치는 경우 AMS는 인프라 복원을 권장합니다. 문제를 해결하거나 알려진 양호한 백업에서 복원하는 사이에는 절충점이 있는 경우가 많으며, 서비스가 가동 중지로 인한 고객 위험과 영향이 결정 요인입니다. 문제 해결에 전념할 시간이 있는 경우 AMS가 도와드릴 것이지만, 복원 긴급성이 높으면 즉시 복원을 시작할 수 있습니다.

Note

스택 템플릿 또는 데이터 복원의 일부가 아닌 임시 데이터는 손실됩니다. AMS는 AWS 서비스 제품을 사용할 수 없는 동안 인프라 복원을 수행하기 위해 합리적인 노력을 기울입니다. AWS 서비스 제품을 사용할 수 있게 되면 인프라 복원이 완료됩니다. AMS에서 권장하는 인프라 복원을 승인하지 않으면 인시던트 해결 시간에 대한 AMS 서비스 약정에 대한 서비스 크레딧을 받을 수 없습니다.

규정 준수 확인

AMS는 AWS Config 규칙 및 수정 작업 라이브러리를 배포하고 관리하여 계정의 보안 및 운영 무결성을 저하시킬 수 있는 잘못된 구성으로부터 보호합니다.

예를 들어 Amazon S3 버킷이 생성되면 Amazon S3 버킷이 퍼블릭 읽기 액세스를 거부해야 하는 규칙을 기준으로 Amazon S3 버킷을 평가할 AWS Config 수 있습니다. Amazon S3 버킷 정책 또는 버킷 액세스 제어 목록(ACL)이 퍼블릭 읽기 액세스를 허용하는 경우는 버킷과 규칙을 모두 미준수로 AWS Config 표시합니다. 이러한 표시는 평가 결과에 따라 리소스를 규정 준수, 규정 미준수 또는 해당 사항

없음으로 AWS Config 규칙 표시합니다. AWS Config 서비스에 대한 자세한 내용은 [AWS Config 개발자 안내서](#)를 참조하세요.

AWS Config 콘솔, AWS CLI 또는 AWS Config API를 사용하여 계정에 배포된 규칙과 규칙 및 리소스의 규정 준수 상태를 볼 수 있습니다. 자세한 내용은 AWS Config 설명서: [구성 규정 준수 보기를 참조하세요](#).

Note

이 주제에 대한 추가 정보는 AWS Artifact 보고서에 액세스하여 확인할 수 있습니다. 자세한 내용은 [AWS Artifact의 보고서 다운로드](#) 섹션을 참조하세요. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 [AWS 아티팩트 시작하기](#)를 참조하세요. 이 정보에는 민감한 보안 콘텐츠가 포함되어 있으므로 이 사용 설명서에 포함되지 않습니다.

의 규정 준수 상태를 보는 다중 계정 랜딩 존 AWS Config 규칙

AMS 다중 계정 AWS Config 랜딩 존은 집계자 서비스를 활용하여 모든 계정에서 규정 준수에 대한 중앙 집중식 보기를 생성합니다. 즉, 보안 계정의 애그리게이터에서 AMS 다중 계정 AWS Config 랜딩 존 환경 AWS Config 규칙 전체의 규정 준수 상태를 확인할 수 있습니다.

다음은 계정 AWS Config 규칙 간 AWS Config의 중앙 규정 준수 상태를 보여주는 집계자의 샘플입니다.

자세한 내용은 [Config Aggregator](#)에 대한 AWS 설명서를 참조하세요.

• AMS는 AWS Config 규칙을 어떻게 사용하나요?

AMS는 규칙에 지정된 조건에 대한 AWS 리소스 구성을 볼 수 AWS Config 규칙 있도록 생성합니다. 규칙이 규정을 준수하지 않는 경우 변경을 요청할 수 있으며 AMS Ops 팀이 사용자와 협력하여 수정 조치를 취합니다.

• 이 경우 AMS 계정에 다음과 같은 변경 사항이 표시됩니다.

- AWS Config 규칙 AWS Config > 규칙에서
- Lambda 함수가 있는 사용자 지정 Config 규칙이 계정에 있습니다.
- 보안 계정의 Config Aggregator 및 모든 계정의 Config Authorization(다중 계정 랜딩 존만 해당)

다음은의 샘플 AWS Config 규칙이며 규정 준수 평가 결과는 다음과 같습니다.

AWS Config에 대한 자세한 내용은 다음을 참조하세요.

- AWS Config: [Config란 무엇입니까?](#)
- AWS Config 규칙: [규칙을 사용하여 리소스 평가](#)
- AWS Config 규칙: [동적 규정 준수 확인: AWS Config 규칙 - 클라우드 리소스에 대한 동적 규정 준수 확인](#)
- AWS Config 집계자: [다중 계정 다중 리전 데이터 집계](#)

AMS 다중 계정 랜딩 존 서비스 제어 정책 제한

이 섹션에는 민감한 AMS 보안 관련 정보가 포함되어 있으므로 수정되었습니다. 이 정보는 AMS 콘솔 설명서를 통해 확인할 수 있습니다. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 [AWS 아티팩트 시작하기](#)를 참조하세요.

복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 지연 시간이 짧고 처리량이 많으며 중복성이 높은 네트워킹과 연결된 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공합니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 [AWS 글로벌 인프라](#)를 참조하세요.

인프라 보안

Note

이 주제에 대한 추가 정보는 AWS Artifact 보고서에 액세스하여 확인할 수 있습니다. 자세한 내용은 [AWS Artifact의 보고서 다운로드](#) 섹션을 참조하세요. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 [AWS 아티팩트 시작하기](#)를 참조하세요. 이 정보에는 민감한 보안 콘텐츠가 포함되어 있으므로 이 사용 설명서에 포함되지 않습니다.

end-of-support 운영 체제에 대한 보안 제어

운영 체제 제조업체의 '지원 end-of-support' 또는 EOS의 일반 지원 기간을 벗어나고 보안 업데이트를 받지 않는 운영 체제는 보안 위험이 증가합니다.

AWS 는 운영 체제 end-of-support를 처리하는 데 도움이 되는 몇 가지 서비스를 제공합니다. Windows end-of-support 대한 자세한 내용은 [Windows ServerEnd-of-Support 마이그레이션 프로그램을 참조하세요](#).

Note

이 주제에 대한 추가 정보는 AWS Artifact 보고서에 액세스하여 확인할 수 있습니다. 자세한 내용은 [AWS Artifact의 보고서 다운로드](#) 섹션을 참조하세요. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 [AWS 아티팩트 시작하기](#)를 참조하세요. 이 정보에는 민감한 보안 콘텐츠가 포함되어 있으므로 이 사용 설명서에 포함되지 않습니다.

보안 그룹 사용

보안 그룹은 하나 이상의 인스턴스에 대한 트래픽을 제어하는 가상 방화벽 역할을 합니다. AMS 보안 그룹을 사용하면 인스턴스 수준에서 인바운드 트래픽 규칙과 아웃바운드 트래픽 규칙을 설정할 수 있습니다. 보안 그룹을 생성하고 AMS 계정, Amazon EC2 인스턴스, Amazon RDS DB 인스턴스, 로드 밸런서, Deep Security Manager(DSM) 복제 인스턴스, EFS 탑재 대상 및 ElastiCache 클러스터에서 보안 그룹과 연결할 리소스를 지정할 수 있습니다. 연결되면 해당 인스턴스와 주고받는 트래픽은 보안 그룹에 설정된 규칙에 의해 제한됩니다.

일반적인 AWS 보안을 더 잘 이해하려면 [보안, 자격 증명 및 규정 준수 모범 사례](#)와 [Linux 인스턴스용 Amazon EC2 보안 그룹을 참조하세요](#).

이제 AMS에 보안 그룹을 생성하고 관리하기 위한 변경 유형 세트가 있습니다.

- 배포 | 고급 스택 구성 요소 | 보안 그룹 | 생성(ct-10xx2g2d7hc90)
- 관리 | 고급 스택 구성 요소 | 보안 그룹 | 삭제(ct-3cp96z7r065e4)
- 관리 | 고급 스택 구성 요소 | 보안 그룹 | 업데이트(ct-3memthlcmvc1b)

예제는 [보안 그룹](#)을 참조하세요.

보안 그룹

AWS VPCs에서 AWS 보안 그룹은 하나 이상의 스택(인스턴스 또는 인스턴스 세트)에 대한 트래픽을 제어하는 가상 방화벽 역할을 합니다. 스택이 시작되면 스택이 하나 이상의 보안 그룹과 연결되어 스택에 도달할 수 있는 트래픽이 결정됩니다.

- 퍼블릭 서브넷의 스택의 경우 기본 보안 그룹은 모든 위치(인터넷)의 HTTP(80) 및 HTTPS(443) 트래픽을 수락합니다. 또한 스택은 회사 네트워크의 내부 SSH 및 RDP 트래픽과 AWS 접속을 허용합니다. 그러면 이러한 스택이 모든 포트를 통해 인터넷으로 나갈 수 있습니다. 또한 프라이빗 서브넷과 퍼블릭 서브넷의 다른 스택으로 나갈 수도 있습니다.
- 프라이빗 서브넷의 스택은 프라이빗 서브넷의 다른 스택으로 송신할 수 있으며, 스택 내의 인스턴스는 모든 프로토콜을 통해 서로 완전히 통신할 수 있습니다.

Important

프라이빗 서브넷의 스택에 대한 기본 보안 그룹을 사용하면 프라이빗 서브넷의 모든 스택이 해당 프라이빗 서브넷의 다른 스택과 통신할 수 있습니다. 프라이빗 서브넷 내의 스택 간 통신을 제한하려면 제한을 설명하는 새 보안 그룹을 생성해야 합니다. 예를 들어 프라이빗 서브넷의 스택이 특정 포트를 통해서만 특정 애플리케이션 서버에서 통신할 수 있도록 데이터베이스 서버와의 통신을 제한하려면 특수 보안 그룹을 요청합니다. 이렇게 하는 방법은 이 단원에서 설명합니다.

기본 보안 그룹

MALZ

다음 표에서는 스택의 기본 인바운드 보안 그룹(SG) 설정을 설명합니다. SG의 이름은 "SentinelDefaultSecurityGroupPrivateOnly-vpc-ID"이며, 여기서 **ID**는 AMS 다중 계정 랜딩 존 계정의 VPC ID입니다. 모든 트래픽은 이 보안 그룹을 통해 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly"로 아웃바운드할 수 있습니다(스택 서브넷 내의 모든 로컬 트래픽 허용).

모든 트래픽은 두 번째 보안 그룹 "SentinelDefaultSecurityGroupPrivateOnly"에 의해 0.0.0.0/0으로 아웃바운드할 수 있습니다.

i Tip

EC2 생성 또는 OpenSearch 생성 도메인과 같은 AMS 변경 유형에 대한 보안 그룹을 선택하는 경우 여기에 설명된 기본 보안 그룹 중 하나 또는 생성한 보안 그룹을 사용합니다. AWS EC2 콘솔 또는 VPC 콘솔에서 VPC당 보안 그룹 목록을 찾을 수 있습니다.

내부 AMS용으로 사용되는 추가 기본 보안 그룹이 있습니다.

AMS 기본 보안 그룹(인바운드 트래픽)

Type	프로토콜	포트 범위	소스
모든 트래픽	모두	모두	SentinelDefaultSecurityGroupPrivateOnly(동일한 보안 그룹의 구성원으로서의 아웃바운드 트래픽 제한)
모든 트래픽	모두	모두	SentinelDefaultSecurityGroupPrivateOnlyEgress All(아웃바운드 트래픽을 제한하지 않음)
HTTP, HTTPS, SSH, RDP	TCP	80/443(소스 0.0.0.0/0) Bastion에서 SSH 및 RDP 액세스 허용	SentinelDefaultSecurityGroupPublic(아웃바운드 트래픽을 제한하지 않음)
MALZ 접속:			
SSH	TCP	22	SharedServices VPC CIDR 및 DMZ VPC CIDR과 고객이 제공한 온프레미스 CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 접속:			
SSH	TCP	22	mc-initial-garden-LinuxBastionSG

Type	프로토콜	포트 범위	소스
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

SALZ

다음 표에서는 스택의 기본 인바운드 보안 그룹(SG) 설정을 설명합니다. SG의 이름은 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly-**ID**"이며, 여기서 **ID**는 고유 식별자입니다. 모든 트래픽은 이 보안 그룹을 통해 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly"로 아웃바운드할 수 있습니다(스택 서브넷 내의 모든 로컬 트래픽 허용).

모든 트래픽은 두 번째 보안 그룹 "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnlyEgressAll-**ID**"에 의해 0.0.0.0/0으로 아웃바운드할 수 있습니다.

Tip

EC2 생성 또는 OpenSearch 생성 도메인과 같은 AMS 변경 유형에 대한 보안 그룹을 선택하는 경우 여기에 설명된 기본 보안 그룹 중 하나 또는 생성한 보안 그룹을 사용합니다. AWS EC2 콘솔 또는 VPC 콘솔에서 VPC당 보안 그룹 목록을 찾을 수 있습니다.

내부 AMS용으로 사용되는 추가 기본 보안 그룹이 있습니다.

AMS 기본 보안 그룹(인바운드 트래픽)

Type	프로토콜	포트 범위	소스
모든 트래픽	모두	모두	SentinelDefaultSecurityGroupPrivateOnly(동일한 보안 그룹의 구성원으로서의 아웃바운드 트래픽 제한)
모든 트래픽	모두	모두	SentinelDefaultSecurityGroupPrivateOnlyEgressAll(아웃바운드 트래픽을 제한하지 않음)

Type	프로토콜	포트 범위	소스
HTTP, HTTPS, SSH, RDP	TCP	80/443(소스 0.0.0.0/0) Bastion에서 SSH 및 RDP 액세스 허용	SentinelDefaultSecurityGroupPublic(아웃바운드 트래픽을 제한하지 않음)
MALZ 접속:			
SSH	TCP	22	SharedServices VPC CIDR 및 DMZ VPC CIDR과 고객이 제공한 온프레미스 CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 접속:			
SSH	TCP	22	mc-initial-garden-LinuxBastionSG
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

보안 그룹 생성, 변경 또는 삭제

사용자 지정 보안 그룹을 요청할 수 있습니다. 기본 보안 그룹이 애플리케이션 또는 조직의 요구 사항을 충족하지 않는 경우 새 보안 그룹을 수정하거나 생성할 수 있습니다. 이러한 요청은 승인 필수로 간주되며 AMS 운영 팀에서 검토합니다.

스택 및 VPCs 외부에서 보안 그룹을 생성하려면 Deployment | Advanced stack components | Security group | Create (review required) 변경 유형(ct-10xx2g2d7hc90)을 사용하여 RFC를 제출합니다.

Active Directory(AD) 보안 그룹 수정의 경우 다음 변경 유형을 사용합니다.

- 사용자를 추가하려면: 관리 | 디렉터리 서비스 | 사용자 및 그룹 | 그룹에 사용자 추가
[ct-24pi85mjtza8k]를 사용하여 RFC 제출
- 사용자를 제거하려면: 관리 | 디렉터리 서비스 | 사용자 및 그룹 | 그룹에서 사용자 제거
[ct-2019s9y3nfm14]를 사용하여 RFC 제출

Note

'검토 필요' CTs를 사용하는 경우 ASAP 예약 옵션(콘솔에서 ASAP 선택, API/CLI에서 시작 및 종료 시간 비워 두기)을 사용하는 것이 좋습니다. 이러한 CTs는 AMS 운영자가 RFC를 검사하고 승인 및 실행 전에 사용자와 통신해야 하기 때문입니다. 이러한 RFCs 예약하는 경우 최소 24시간을 허용해야 합니다. 예정된 시작 시간 전에 승인이 이루어지지 않으면 RFC가 자동으로 거부됩니다.

보안 그룹 찾기

스택 또는 인스턴스에 연결된 보안 그룹을 찾으려면 EC2 콘솔을 사용합니다. 스택 또는 인스턴스를 찾은 후 스택 또는 인스턴스에 연결된 모든 보안 그룹을 볼 수 있습니다.

명령줄에서 보안 그룹을 찾고 출력을 필터링하는 방법은 섹션을 참조하세요 [describe-security-groups](#).

AMS 예방 및 탐지 제어 라이브러리

AWS Managed Services(AMS)는 AMS 계정의 보안 태세를 개선하고 규정 준수 격차를 완화하는 데 활용할 수 있는 검증된 서비스 제어 정책(SCPs) 및 ConfigRules의 업선된 라이브러리/카탈로그를 제공합니다.

주제

- [큐레이션SCPs 및 구성 규칙](#)
- [Config 규칙에 대한 사용자 지정 알림](#)

큐레이션SCPs 및 구성 규칙

AMS Advanced에 대해 큐레이션된 SCPs 및 구성 규칙.

- 서비스 제어 정책(SCPs): 제공된 SCPs는 기본 AMS 정책에 추가됩니다.

이러한 라이브러리 컨트롤을 기본 컨트롤과 함께 사용하여 특정 보안 요구 사항을 충족할 수 있습니다.

- 구성 규칙: AMS는 기본 AMS 구성 규칙(기본 규칙은 AMS 아티팩트 참조) 외에도 적합성 팩(AWS Config 안내서의 [적합성 팩](#) 참조)을 적용할 것을 권장합니다. 적합성 팩은 대부분의 규정 준수 요구 사항을 다루며 AWS는 이를 정기적으로 업데이트합니다.

여기에 나열된 규칙을 사용하여 적합성 팩에서 다루지 않는 사용 사례별 격차를 해결할 수 있습니다.

Note

AMS 기본 규칙 및 적합성 팩이 시간이 지남에 따라 업데이트되면 이러한 규칙이 중복될 수 있습니다.

AMS는 일반적으로 중복 Config 규칙을 정기적으로 정리할 것을 권장합니다.

AMS Advanced의 경우 Config 규칙은 out-of-band 변경을 방지하기 위해 자동 문제 해결([AWS Config 규칙에 의한 규정 미준수 AWS 리소스 문제 해결](#) 참조)을 사용해서는 안 됩니다.

SCP-AMS-001: EBS 생성 제한

암호화가 활성화되지 않은 경우 EBS 볼륨 생성을 방지합니다.

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:CreateVolume",
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-002: EC2 시작 제한

EBS 볼륨이 암호화되지 않은 경우 EC2 인스턴스가 시작되지 않도록 합니다. 여기에는 암호화되지 않은 AMIs에서 EC2 시작을 거부하는 것이 포함됩니다. 이 SCP는 루트 볼륨에도 적용되기 때문입니다.

```
{
  "Condition": {
```

```

    "Bool": {
      "ec2:Encrypted": "false"
    },
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:volume/*",
    "Effect": "Deny"
  }
}

```

SCP-ADV-001: RFC 제출 제한

기본 AMS 역할이 VPC RFCs를 제출하지 못하도록 제한합니다. 이는 페더레이션 역할에 더 세분화된 권한을 적용하려는 경우에 유용합니다.

예를 들어 VPC AWSManagedServicesChangeManagement Role 생성 및 삭제, 추가 서브넷 생성, 애플리케이션 계정 오프보딩, SAML 자격 증명 공급자 업데이트 또는 삭제를 허용하는 RFC를 제외한 대부분의 사용 가능한 RFC를 기본값으로 제출할 수 있습니다. RFCs

SCP-AMS-003: AMS에서 EC2 또는 RDS 생성 제한

AMS 기본 AMS Backup IAM 역할이 그렇게 하도록 허용하면서 특정 태그가 없는 Amazon EC2 및 RDS 인스턴스의 생성을 방지합니다. 이는 재해 복구 또는 DR에 필요합니다.

```

{
  "Sid": "DenyRunInstanceWithNoOrganizationTag",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances",
    "rds:CreateDBInstance"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:rds:*:*:db:*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/organization": "true"
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::<Account_Number>:role/ams-backup-iam-role"
      ]
    }
  }
}

```

```

    }
  }
}

```

SCP-AMS-004: S3 업로드 제한

암호화되지 않은 S3 객체의 업로드를 방지합니다.

```

{
    "Sid": "DenyUnencryptedS3Uploads",
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
        "StringNotLike": {
            "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"]
        },
        "Null": {
            "s3:x-amz-server-side-encryption": "false"
        }
    }
}

```

SCP-AMS-005: API 및 콘솔 액세스 제한

확인된 고객 InfoSec에 따라 알려진 잘못된 IP 주소에서 오는 요청에 대한 AWS 콘솔 및 API 액세스를 방지합니다.

SCP-AMS-006: IAM 엔터티가 조직에서 멤버 계정을 제거하지 못하도록 방지

AWS Identity and Access Management 엔터티가 조직에서 멤버 계정을 제거하지 못하도록 합니다.

```

{
    "Effect": "Deny",
    "Action": ["organizations:LeaveOrganization"],
    "Resource": ["*"]
}

```

SCP-AMS-007: 조직 외부의 계정에 리소스 공유 방지

AWS 조직 외부의 외부 계정과 리소스 공유 방지

```
{
  "Effect": "Deny",
  "Action": [
    "ram:*"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "Bool": {
      "ram:AllowsExternalPrincipals": "true"
    }
  }
},
{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
    "ram:UpdateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "ram:RequestedAllowsExternalPrincipals": "true"
    }
  }
}
```

SCP-AMS-008: 조직 또는 조직 단위(OU)와의 공유 방지

조직에 있는 계정 및/또는 OU와의 리소스 공유를 방지합니다.

```
{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
    "ram:AssociateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringLike": {
      "ram:Principal": [
```

```

        "arn:aws:organizations::*:account/o-${OrganizationId}/${AccountId}",
        "arn:aws:organizations::*:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}"
    ]
}
}
}

```

SCP-AMS-009: 사용자가 리소스 공유 초대를 수락하지 못하도록 방지

멤버 계정이 리소스 공유에 가입 AWS RAM 하기 위한의 초대를 수락하지 못하도록 합니다. 이 API는 조건을 지원하지 않으며 외부 계정의 공유만 방지합니다.

```

{
  "Effect": "Deny",
  "Action": ["ram:AcceptResourceShareInvitation"],
  "Resource": ["*"]
}

```

SCP-AMS-010: 계정 리전 활성화 및 비활성화 작업 방지

AWS 계정에 대해 새 AWS 리전을 활성화하거나 비활성화하지 마십시오.

```

{
  "Effect": "Deny",
  "Action": [
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource": "*"
}

```

SCP-AMS-011: 결제 수정 작업 방지

결제 및 결제 구성에 대한 수정을 방지합니다.

```

{
  "Effect": "Deny",
  "Action": [
    "aws-portal:ModifyBilling",
    "aws-portal:ModifyAccount",
    "aws-portal:ModifyPaymentMethods"
  ],
}

```

```
"Resource": "*"
}
```

SCP-AMS-012: 특정 CloudTrails 대한 삭제 또는 수정 방지

특정 AWS CloudTrail 추적에 대한 수정을 방지합니다.

```
{
  "Effect": "Deny",
  "Action": [
    "cloudtrail:DeleteEventDataStore",
    "cloudtrail:DeleteTrail",
    "cloudtrail:PutEventSelectors",
    "cloudtrail:PutInsightSelectors",
    "cloudtrail:UpdateEventDataStore",
    "cloudtrail:UpdateTrail",
    "cloudtrail:StopLogging"
  ],
  "Resource": [
    "arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}"
  ]
}
```

SCP-AMS-013: 기본 EBS 암호화 비활성화 방지

기본 Amazon EBS 암호화의 비활성화를 방지합니다.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

SCP-AMS-014: 기본 VPC 및 서브넷 생성 방지

기본 Amazon VPC 및 서브넷의 생성을 방지합니다.

```
{
  "Effect": "Deny",
  "Action": [
```



```
"ec2:CreateDefaultSubnet",
"ec2:CreateDefaultVpc"
],
"Resource": "*"
}
```

SCP-AMS-015: GuardDuty 비활성화 및 수정 방지

Amazon GuardDuty가 수정되거나 비활성화되지 않도록 합니다.

```
{
  "Effect": "Deny",
  "Action": [
    "guardduty:AcceptInvitation",
    "guardduty:ArchiveFindings",
    "guardduty:CreateDetector",
    "guardduty:CreateFilter",
    "guardduty:CreateIPSet",
    "guardduty:CreateMembers",
    "guardduty:CreatePublishingDestination",
    "guardduty:CreateSampleFindings",
    "guardduty:CreateThreatIntelSet",
    "guardduty:DeclineInvitations",
    "guardduty>DeleteDetector",
    "guardduty>DeleteFilter",
    "guardduty>DeleteInvitations",
    "guardduty>DeleteIPSet",
    "guardduty>DeleteMembers",
    "guardduty>DeletePublishingDestination",
    "guardduty>DeleteThreatIntelSet",
    "guardduty:DisableOrganizationAdminAccount",
    "guardduty:DisassociateFromMasterAccount",
    "guardduty:DisassociateMembers",
    "guardduty:InviteMembers",
    "guardduty:StartMonitoringMembers",
    "guardduty:StopMonitoringMembers",
    "guardduty:TagResource",
    "guardduty:UnarchiveFindings",
    "guardduty:UntagResource",
    "guardduty:UpdateDetector",
    "guardduty:UpdateFilter",
    "guardduty:UpdateFindingsFeedback",
    "guardduty:UpdateIPSet",
    "guardduty:UpdateMalwareScanSettings",
  ]
}
```

```

    "guardduty:UpdateMemberDetectors",
    "guardduty:UpdateOrganizationConfiguration",
    "guardduty:UpdatePublishingDestination",
    "guardduty:UpdateThreatIntelSet"
  ],
  "Resource": "*"
}
```

SCP-AMS-016: 루트 사용자 활동 방지

루트 사용자가 작업을 수행하지 못하도록 합니다.

```

{
  "Action": "*",
  "Resource": "*",
  "Effect": "Deny",
  "Condition": {
    "StringLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::*:root"
      ]
    }
  }
}
```

SCP-AMS-017: 루트 사용자에게 액세스 키 생성 방지

루트 사용자의 액세스 키 생성을 방지합니다.

```

{
  "Effect": "Deny",
  "Action": "iam:CreateAccessKey",
  "Resource": "arn:aws:iam::*:root"
}
```

SCP-AMS-018: S3 계정 퍼블릭 액세스 블록 비활성화 방지

Amazon S3 계정 퍼블릭 액세스 블록의 비활성화를 방지합니다. 이렇게 하면 계정의 버킷이 공개되지 않습니다.

```

{
  "Effect": "Deny",
```

```
"Action": "s3:PutAccountPublicAccessBlock",
"Resource": "*"
}
```

SCP-AMS-019: AWS Config 비활성화 또는 Config 규칙 수정 방지

AWS Config 규칙 비활성화 또는 수정을 방지합니다.

```
{
  "Effect": "Deny",
  "Action": [
    "config:DeleteConfigRule",
    "config:DeleteConfigurationRecorder",
    "config:DeleteDeliveryChannel",
    "config:DeleteEvaluationResults",
    "config:StopConfigurationRecorder"
  ],
  "Resource": "*"
}
```

SCP-AMS-020: 모든 IAM 작업 방지

모든 IAM 작업을 방지합니다.

```
{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": "*"
}
```

SCP-AMS-021: CloudWatch Logs 그룹 및 스트림 삭제 방지

Amazon CloudWatch Logs 그룹 및 스트림 삭제를 방지합니다.

```
{
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
}
```

```
"Resource": "*"
}
```

SCP-AMS-022: Glacier 삭제 방지

Amazon Glacier 삭제를 방지합니다.

```
{
  "Effect": "Deny",
  "Action": [
    "glacier:DeleteArchive",
    "glacier:DeleteVault"
  ],
  "Resource": "*"
}
```

SCP-AMS-023: IAM Access Analyzer 삭제 방지

IAM Access Analyzer의 삭제를 방지합니다.

```
{
  "Action": [
    "access-analyzer:DeleteAnalyzer"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-024: Security Hub 수정 방지

삭제를 방지합니다 AWS Security Hub.

```
{
  "Action": [
    "securityhub:DeleteInvitations",
    "securityhub:DisableSecurityHub",
    "securityhub:DisassociateFromMasterAccount",
    "securityhub:DeleteMembers",
    "securityhub:DisassociateMembers"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

```
}
```

SCP-AMS-025: 디렉터리 서비스에서 삭제 방지

아래의 리소스 삭제를 방지합니다 AWS Directory Service.

```
{
  "Action": [
    "ds:DeleteDirectory",
    "ds:DeleteLogSubscription",
    "ds:DeleteSnapshot",
    "ds:DeleteTrust",
    "ds:DeregisterCertificate",
    "ds:DeregisterEventTopic",
    "ds:DisableLDAPS",
    "ds:DisableRadius",
    "ds:DisableSso",
    "ds:UnshareDirectory"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-026: 거부된 서비스 사용 방지

거부된 서비스의 사용을 방지합니다.

Note

service1 및 *service2*를 서비스 이름으로 바꿉니다. *access-analyzer* 또는 *IAM*의 예입니다.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"]
}
```

SCP-AMS-027: 특정 리전에서 거부된 서비스 사용 방지

특정 AWS 리전에서 거부된 서비스의 사용을 방지합니다.

Note

service1 및 *service2*를 서비스 이름으로 바꿉니다. *access-analyzer* 또는 *IAM*의 예입니다.

region1 및 *region2*를 서비스 이름으로 바꿉니다. *us-west-2* 또는 *use-east-1*의 예입니다.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"],
  "Condition": {
    "StringEquals": {
      "aws:RequestedRegion": [
        "region1",
        "region2"
      ]
    }
  }
}
```

SCP-AMS-028: 승인된 보안 주체를 제외한 태그 수정 방지

승인된 보안 주체를 제외한 모든 사용자의 태그 수정을 방지합니다. 권한 부여 태그를 사용하여 보안 주체에 권한을 부여합니다. 권한 부여 태그는 리소스 및 보안 주체와 연결되어야 합니다. 사용자/역할은 리소스와 보안 주체의 태그가 모두 일치하는 경우에만 승인된 것으로 간주됩니다. 자세한 정보는 다음 자료를 참조하세요.

- [의 서비스 제어 정책을 사용하여 권한 부여에 사용되는 리소스 태그 보호 AWS Organizations](#)
- [승인된 보안 주체를 제외한 태그 수정 방지](#)

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource": [
```

```
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
    },
    "Null": {
      "ec2:ResourceTag/access-project": false
    }
  }
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
    },
    "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
        "access-project"
      ]
    }
  }
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
```

```

    "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
  },
  "Null": {
    "aws:PrincipalTag/access-project": true
  }
}
}

```

SCP-AMS-029: 사용자가 Amazon VPC 흐름 로그를 삭제하지 못하도록 방지

Amazon VPC 흐름 로그의 삭제를 방지합니다.

```

{
  "Action": [
    "ec2:DeleteFlowLogs",
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:PutLifecycleConfiguration",
    "firehose:DeleteDeliveryStream"
  ],
  "Resource": "*",
  "Effect": "Deny"
}

```

SCP-AMS-030: 네트워크 계정 이외의 계정과 VPC 서브넷 공유 방지

네트워크 계정이 아닌 다른 계정과 Amazon VPC 서브넷을 공유하는 것을 방지합니다.

Note

NETWORK_ACCOUNT_ID를 네트워크 계정 ID로 바꿉니다.

```

{
  "Effect": "Deny",
  "Action": [
    "ram:AssociateResourceShare",
    "ram:CreateResourceShare"
  ],

```



```

"Resource": "*",
"Condition": {
  "StringNotEquals": {
    "ram:Principal": "NETWORK_ACCOUNT_ID"
  },
  "StringEquals": {
    "ram:RequestedResourceType": "ec2:Subnet"
  }
}
}

```

SCP-AMS-031: 금지된 인스턴스 유형으로 인스턴스 시작 방지

금지된 Amazon EC2 인스턴스 유형이 출시되지 않도록 합니다.

Note

instance_type1 및 *instance_type2*를 *t2.micro*와 같이 제한하려는 인스턴스 유형 또는 **.nano*와 같은 와일드카드 문자열로 바꿉니다.

```

{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "ForAnyValue:StringLike": {
      "ec2:InstanceType": [
        "instance_type1",
        "instance_type2"
      ]
    }
  }
}

```

SCP-AMS-032: IMDSv2 없이 인스턴스 시작 방지

IMDSv2 없이 Amazon EC2 인스턴스를 방지합니다. IMDSv2

[

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*"
  }
]
```

SCP-AMS-033: 특정 IAM 역할에 대한 수정 방지

지정된 IAM 역할에 대한 수정을 방지합니다.

```
{
  "Action": [
    "iam:AttachRolePolicy",
```

```

    "iam:DeleteRole",
    "iam:DeleteRolePermissionsBoundary",
    "iam:DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:PutRolePermissionsBoundary",
    "iam:PutRolePolicy",
    "iam:TagRole",
    "iam:UntagRole",
    "iam:UpdateAssumeRolePolicy",
    "iam:UpdateRole",
    "iam:UpdateRoleDescription"
  ],
  "Resource": [
    "arn:aws:iam::{\ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}

```

SCP-AMS-034: 특정 IAM 역할에 대한 AssumeRolePolicy 수정 방지

지정된 IAM 역할에 대한 AssumeRolePolicy 수정을 방지합니다.

```

{
  "Action": [
    "iam:UpdateAssumeRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::{\ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}

```

ConfigRule: 필수 태그

EC2 인스턴스에 필요한 사용자 지정 태그가 있는지 확인합니다. InfoSec 외에도 Cost Management에도 유용합니다.

```

ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the required tags.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'

```

```
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS
  SourceIdentifier: REQUIRED_TAGS
```

ConfigRule: 액세스 키 교체됨

지정된 기간 내에 액세스 키가 교체되고 있는지 확인합니다. 이는 일반적으로 일반적인 규정 준수 요구 사항에 따라 90일로 설정됩니다.

```
ConfigRuleName: access-keys-rotated
Description: >-
  A config rule that checks whether the active access keys are rotated
  within the number of days specified in maxAccessKeyAge. The rule is
  NON_COMPLIANT if the access keys have not been rotated for more than
  maxAccessKeyAge number of days.
InputParameters:
  maxAccessKeyAge: '90'
Source:
  Owner: AWS
  SourceIdentifier: ACCESS_KEYS_ROTATED
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: AMS의 IAM 루트 액세스 키

루트 액세스 키가 계정에 없는지 확인합니다. AMS Advanced 계정의 경우 기본적으로 규정을 준수할 것으로 예상됩니다 out-of-the-box.

```
ConfigRuleName: iam-root-access-key-check
Description: >-
  A config rule that checks whether the root user access key is available. The
  rule is COMPLIANT if the user access key does not exist.
Source:
  Owner: AWS
  SourceIdentifier: IAM_ROOT_ACCESS_KEY_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: SSM 관리형 EC2

SSM Systems Manager에서 EC2s 관리하고 있는지 확인합니다.

```
ConfigRuleName: ec2-instance-managed-by-systems-manager
Description: >-
  A Config rule that checks whether the EC2 instances in the
  account are managed by AWS Systems Manager.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
    - 'AWS::SSM::ManagedInstanceInventory'
Source:
  Owner: AWS
  SourceIdentifier: EC2_INSTANCE_MANAGED_BY_SSM
```

ConfigRule: AMS에서 미사용 IAM 사용자

지정된 기간 동안 사용되지 않은 IAM 사용자 자격 증명을 확인합니다. 키 교체 확인과 마찬가지로 일반적으로 일반적인 규정 준수 요구 사항에 따라 기본값은 90일입니다.

```
ConfigRuleName: iam-user-unused-credentials-check
Description: >-
  A config rule that checks whether IAM users have passwords
  or active access keys that have not been used within the
  specified number of days provided.
InputParameters:
  maxCredentialUsageAge: '90'
Source:
  Owner: AWS
SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: S3 버킷 로깅

계정의 S3 버킷에 대해 로깅이 활성화되었는지 확인합니다.

```
ConfigRuleName: s3-bucket-logging-enabled
Description: >-
  A Config rule that checks whether logging is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_LOGGING_ENABLED
```

ConfigRule: S3 버킷 버전 관리

모든 S3 버킷에서 버전 관리 및 MFA 삭제(선택 사항)가 활성화되어 있는지 확인합니다.

```
ConfigRuleName: s3-bucket-versioning-enabled
Description: >-
  A Config rule that checks whether versioning is enabled for S3
  buckets. Optionally, the rule checks if MFA delete is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED
```

ConfigRule: S3 퍼블릭 액세스

퍼블릭 액세스 설정(퍼블릭 ACL, 퍼블릭 정책, 퍼블릭 버킷)이 계정 전체에서 제한되는지 확인합니다.

```
ConfigRuleName: s3-account-level-public-access-blocks
Description: >-
  A Config rule that checks whether the required public access block
  settings are configured from account level. The rule is only
  NON_COMPLIANT when the fields set below do not match the corresponding
  fields in the configuration item.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::AccountPublicAccessBlock'
InputParameters:
  IgnorePublicAcls: 'True'
  BlockPublicPolicy: 'True'
  BlockPublicAcls: 'True'
  RestrictPublicBuckets: 'True'
Source:
  Owner: AWS
SourceIdentifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
```

ConfigRule: 보관되지 않은 GuardDuty 조사 결과

지정된 기간보다 오래된 보관되지 않은 GuardDuty 결과가 있는지 확인합니다. 기본 기간은 Low-sev의 경우 30일, Medium-sev의 경우 7일, High-sev 결과의 경우 1일입니다.

```
ConfigRuleName: guardduty-non-archived-findings
```

```
Description: >-
  A Config rule that checks whether the Amazon GuardDuty has findings that
  are non archived. The rule is NON_COMPLIANT if GuardDuty has non
  archived low/medium/high severity findings older than the specified number.
InputParameters:
  daysLowSev: '30'
  daysMediumSev: '7'
  daysHighSev: '1'
Source:
  Owner: AWS
  SourceIdentifier: GUARDDUTY_NON_ARCHIVED_FINDINGS
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: CMK 삭제

삭제가 예약된(일명 보류 중) AWS Key Management Service 사용자 지정 마스터 키(CMKs)가 있는지 확인합니다. 이는 CMK 삭제를 인식하지 못하면 데이터를 복구할 수 없게 될 수 있으므로 중요합니다.

```
ConfigRuleName: kms-cmk-not-scheduled-for-deletion
Description: >-
  A config rule that checks whether customer master keys (CMKs) are not
  scheduled for deletion in AWS Key Management Service (AWS KMS). The rule is
  NON_COMPLIANT if CMKs are scheduled for deletion.
Source:
  Owner: AWS
SourceIdentifier: KMS_CMK_NOT_SCHEDULED_FOR_DELETION
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: CMK 교체

계정의 모든 CMK에 대해 자동 교체가 활성화되어 있는지 확인

```
ConfigRuleName: cmk-backing-key-rotation-enabled
Description: >-
  A config rule that checks that key rotation is enabled for each customer
  master key (CMK). The rule is COMPLIANT, if the key rotation is enabled
  for specific key object. The rule is not applicable to CMKs that have
  imported key material.
Source:
  Owner: AWS
SourceIdentifier: CMK_BACKING_KEY_ROTATION_ENABLED
MaximumExecutionFrequency: TwentyFour_Hours
```

Config 규칙에 대한 사용자 지정 알림

InfoSec 및 리더십 팀에 직접 에스컬레이션된 인식을 높여야 하는 규정을 준수하지 않는 중요한 Config 규칙이 발생할 수 있습니다. 이러한 시나리오의 경우 AMS는 규정 미준수 이벤트 기반 사용자 지정 알림을 구성할 것을 권장합니다.

예:

```
ConfigRuleName: required-tags
  Description: >-
    A Config rule that checks whether EC2 instances have the mandated tags.
  Scope:
    ComplianceResourceTypes:
      - 'AWS::EC2::Instance'
  InputParameters:
    tag1Key: COST_CENTER
    tag2Key: APP_ID
  Source:
    Owner: AWS
SourceIdentifier: REQUIRED_TAGS
NotificationEventRule:
  Type: 'AWS::Events::Rule'
  Properties:
    Name: CWEventForrequired-tags
    Description: >-
      SNS Notification for Non-Compliant Events of Config Rule:
      required-tags
    State: ENABLED
    EventPattern:
      detail-type:
        - Config Rules Compliance Change
      source:
        - aws.config
      detail:
        newEvaluationResult:
          complianceType:
            - NON_COMPLIANT
        configRuleARN:
          - 'Fn::GetAtt':
              - RequiredEC2Tags
              - Arn
    Targets:
      - Id: RemediationNotification
```



```
    Arn:
      Ref: SnsTopic
    InputTransformer:
      InputTemplate: >-
        "EC2 Instance <Instance_ID> is non-compliant. Please add required tags:
        COST_CENTER, APP_ID, Name, and Backup."
      InputPathsMap:
        instance_id: $.detail.resourceId
  SnsTopic:
    Type: 'AWS::SNS::Topic'
    Properties:
      Subscription:
        - Endpoint: Cloud_Ops_Leaders@customer.com
          Protocol: email
      TopicName: noncompliant-instance-notification
  SnsTopicPolicy:
    Type: 'AWS::SNS::TopicPolicy'
    Properties:
      PolicyDocument:
        Statement:
          - Sid: __default_statement_ID
            Effect: Allow
            Principal:
              AWS: '*'
            Action:
              - 'SNS:GetTopicAttributes'
              - 'SNS:SetTopicAttributes'
              - 'SNS:AddPermission'
              - 'SNS:RemovePermission'
              - 'SNS:DeleteTopic'
              - 'SNS:Subscribe'
              - 'SNS:ListSubscriptionsByTopic'
              - 'SNS:Publish'
              - 'SNS:Receive'
            Resource:
              Ref: SnsTopic
          Condition:
            StringEquals:
              'AWS:SourceOwner':
                Ref: 'AWS::AccountId'
          - Sid: TrustCWEToPublishEventsToMyTopic
            Effect: Allow
            Principal:
              Service: events.amazonaws.com
```

```
Action: 'sns:Publish'
Resource:
  Ref: SnsTopic
Topics:
  - Ref: SnsTopic
```

AMS Advanced에 대한 Amazon EventBridge 규칙 서비스 연결 역할

AMS Advanced는 AWSServiceRoleForManagedServices_Events라는 서비스 연결 역할(SLR)을 사용합니다. 이 역할은 AWS 관리형 서비스 서비스 보안 주체(events.managedservices.amazonaws.com) 중 하나를 신뢰하여 역할을 수입합니다. 서비스는 역할을 사용하여 EventBridge 관리형 규칙을 생성합니다. 이 규칙은 AWS 계정에서 AWS 관리형 서비스로 경보 상태 변경 정보를 전달하는 데 필요한 인프라입니다.

AMS Advanced용 EventBridge SLR에 대한 권한

AWSServiceRoleForManagedServices_Events 서비스 연결 역할은 역할을 수입하기 위해 다음 서비스를 신뢰합니다.

- events.managedservices.amazonaws.com

이 역할에는 AWSManagedServices_EventsServiceRolePolicy AWS 관리형 정책이 연결되어 있습니다([AWS 관리형 정책: AWSManagedServices_EventsServiceRolePolicy](#) 참조). 서비스는 역할을 사용하여 계정의 경보 상태 변경 정보를 관리형 AWS 서비스로 전달합니다. IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [서비스 연결 역할 권한을 참조하세요](#).

이 ZIP: EventsServiceRolePolicy.zip에서 JSON AWSManagedServices_EventsServiceRolePolicy를 다운로드할 수 있습니다. [EventsServiceRolePolicy.zip](#)

AMS Advanced용 EventBridge SLR 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS 관리 콘솔 AWS CLI, 또는 AWS API에서 AMS에 온보딩하면 AMS Advanced가 서비스 연결 역할을 생성합니다.

Important

이 서비스 연결 역할은 2023년 2월 7일 이전에 AMS Advanced 서비스를 사용하던 경우 계정에 나타날 수 있습니다. 서비스 연결 역할을 지원하기 시작한 후 AMS Accelerate가 계정에

AWSServiceRoleForManagedServices_Events 역할을 생성했습니다. 자세한 내용은 [내 IAM 계정에 표시되는 새 역할](#)을 참조하세요.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. AMS에 온보딩하면 AMS Advanced가 서비스 연결 역할을 다시 생성합니다.

AMS Advanced용 EventBridge SLR 편집

AMS Advanced에서는 AWSServiceRoleForManagedServices_Events 서비스 연결 역할을 편집할 수 없습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 편집](#)을 참조하세요.

AMS Advanced용 EventBridge SLR 삭제

AWSServiceRoleForManagedServices_Events 역할은 수동으로 삭제할 필요가 없습니다. AWS 관리 콘솔, AWS CLI 또는 AWS API의 AMS에서 오프보딩하면 AMS Advanced가 리소스를 정리하고 서비스 연결 역할을 삭제합니다.

IAM 콘솔, AWS CLI 또는 AWS API를 사용하여 서비스 연결 역할을 수동으로 삭제할 수도 있습니다. 단, 서비스 연결 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

Note

리소스를 삭제하려고 할 때 AMS Advanced 서비스가 역할을 사용하는 경우 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForManagedServices_Events 서비스 연결 역할에서 사용하는 AMS Advanced 리소스를 삭제하려면

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔, AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForManagedServices_Events 서비스 연결 역할을 삭제합니다.

자세한 내용은 IAM 사용 설명서에서 [서비스 연결 역할 삭제](#)를 참조하세요.

보안 모범 사례

이 섹션에는 민감한 AMS 보안 관련 정보가 포함되어 있으므로 수정되었습니다. 이 정보는 AMS 콘솔 설명서를 통해 확인할 수 있습니다. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 [AWS 아티팩트 시작하기를](#) 참조하세요.

AMS 다중 계정 랜딩 존 EPS 기본값이 아닌 설정

이 섹션에는 민감한 AMS 보안 관련 정보가 포함되어 있으므로 수정되었습니다. 이 정보는 AMS 콘솔 설명서를 통해 확인할 수 있습니다. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 [AWS 아티팩트 시작하기를](#) 참조하세요.

AMS 가드레일

가드레일은 전체 AMS 환경에 대한 지속적인 거버넌스를 제공하는 상위 수준 규칙입니다.

이 섹션에는 민감한 AMS 보안 관련 정보가 포함되어 있으므로 수정되었습니다. 이 정보는 AMS 콘솔 설명서를 통해 확인할 수 있습니다. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 [AWS 아티팩트 시작하기를](#) 참조하세요.

MALZ 서비스 제어 정책

이 섹션에는 민감한 AMS 보안 관련 정보가 포함되어 있으므로 수정되었습니다. 이 정보는 AMS 콘솔 설명서를 통해 확인할 수 있습니다. AWS 아티팩트에 액세스하려면 CSDM에 문의하여 지침을 받거나 [AWS 아티팩트 시작하기를](#) 참조하세요.

AMS의 보안 인시던트 대응

AWS Managed Services(AMS)에서는 보안이 최우선 순위입니다. AMS는 리소스와 제어를 계정에 배포하여 관리합니다. AWS에는 공동 책임 모델이 있습니다. 클라우드의 보안을 AWS 관리하며 사용자는 클라우드의 보안을 책임집니다. AMS는 보안 제어 및 보안 문제에 대한 활성 모니터링을 사용하여 데이터와 자산을 보호하고 AWS 인프라를 안전하게 유지하는 데 도움이 됩니다. 이러한 기능은 AWS 클라우드에서 실행되는 애플리케이션의 보안 기준을 설정하는 데 도움이 됩니다. AMS는 보안 인시던트 대응을 통해 고객과 협력하여 효과를 평가한 다음 모범 사례 권장 사항에 따라 억제 및 수정을 수행합니다.

잘못된 구성이나 외부 요인의 변경으로 인해 기준에서 벗어나는 경우 대응하고 조사해야 합니다. 이를 성공적으로 수행하려면 AMS 환경 내에서 보안 인시던트 대응의 기본 개념을 이해해야 합니다. 또한

보안 문제가 발생하기 전에 클라우드 팀을 준비, 교육 및 훈련하기 위한 요구 사항을 이해해야 합니다. 사용할 수 있는 제어 및 기능을 파악하고, 사용자 계정 손상 또는 권한 있는 계정의 오용과 같은 일반적인 보안 문제에 대한 대응 계획을 준비하고, 자동화를 사용하여 대응 속도와 일관성을 개선하는 해결 방법을 식별하는 것이 중요합니다. 또한 이러한 요구 사항을 충족하기 위한 보안 인시던트 대응 프로그램 구축과 관련된 규정 준수 및 규제 요구 사항을 이해해야 합니다.

보안 인시던트 대응은 복잡할 수 있지만 반복적인 접근 방식을 구현하면 프로세스를 간소화하고 인시던트 대응 팀이 조기 및 지속적인 탐지 및 대응을 제공하여 자산 이해관계자를 만족시킬 수 있습니다. 이 가이드에서는 AMS가 인시던트 대응에 사용하는 방법론, AMS 책임 매트릭스(RACI), 보안 이벤트에 대비하는 방법, 보안 인시던트 발생 시 AMS를 참여시키는 방법, AMS가 사용하는 일부 인시던트 대응 런북을 제공합니다.

AMS 보안 인시던트 대응 작동 방식

AWS Managed Services는 [보안 인시던트 대응을 위한 NIST 800-61 컴퓨터 보안 인시던트 처리 안내서](#)에 부합합니다. 이 업계 표준에 따라 보안 이벤트 관리에 대한 일관된 접근 방식을 제공하고 클라우드의 보안 인시던트를 보호하고 이에 대응하는 모범 사례를 준수합니다.

인시던트 대응 수명 주기

탐지에서 보안 알림을 식별 및 생성하거나 사용자가 보안 지원을 요청할 때 AWS Managed Services Operations 팀은 적시에 조사하고, 자동화를 실행하여 데이터 수집을 수행하고, 분류 및 분석하고, 분석을 알리고, 조사 및 억제 활동을 수행하고, 이벤트 분석을 게시합니다.

인시던트 대응 중에 수행되는 데이터 수집, 분류, 분석 및 억제 활동은 조사 중인 보안 이벤트 유형에 따라 달라집니다. 일부 시나리오에 대한 보안 인시던트 대응 워크플로의 예는 이 문서의 끝에 있습니다.

인시던트 발생 시 AMS는 올바른 조치를 동적으로 결정하므로 문서화된 단계를 적절하게 재정렬하거나 우회하여 올바른 결과가 발생하도록 할 수 있습니다.

준비

위협 환경이 발전함에 따라 AMS는 탐지 및 대응 기능을 계속 확장하고 있습니다. 새로운 탐지가 추가 되면 AMS는 이러한 새로운 탐지의 알림을 탐지 및 대응 플랫폼에 통합합니다. AMS 보안 대응 담당자는 보안 인시던트 대응 수명 주기 전반에 걸쳐 조사하고 협력하도록 훈련됩니다.

이러한 파트너십 접근 방식 때문에 보안 및 애플리케이션 팀이 AMS와 협력하여 이러한 이벤트가 발생할 때 보안 이벤트를 처리할 준비가 되어 있어야 합니다. 이 설명서에서는 보안 이벤트 중에 예상되는 사항을 설명하고 보안 인시던트가 발생할 때 신속한 대응을 준비하는 데 도움이 됩니다.

이 설명서에서는 이벤트의 NIST 800-61 정의를 시스템 또는 네트워크에서 관찰 가능한 발생으로 사용하고 인시던트를 정책, 허용 가능한 사용 정책 또는 표준 보안 관행 위반의 위반 또는 임박한 위협으로 사용합니다.

준비 체크리스트

AMS 클라우드 솔루션 제공 관리자(CSDM) 및 AMS 클라우드 아키텍트(CA)와 함께 다음 체크리스트를 살펴봅니다.

- 어떤 워크로드가 어떤 계정에서 실행되고 있는지 이해합니다.
- 다양한 워크로드를 담당하는 내부 팀을 이해하고 워크로드에서 적절하게 태그를 지정합니다.
- 보안 이벤트 조사 중에 필요할 수 있는 다른 팀과 억제 결정을 위해 연락처 세부 정보를 내부적으로 유지 관리합니다.
- 보안 연락처가 최신 상태이고 모든 관리형 AWS 계정에 추가되었는지 확인합니다. 연락처는 계정별로 관리됩니다.
- 보안 인시던트를 AMS에 제기하는 방법을 알고 심각도와 예상 대응 시간을 숙지합니다.
- 보안 알림이 수신되면 페이지어 또는 보안 운영 센터와 같은 적절한 사람과 시스템으로 라우팅되어야 합니다.
- 사용 가능한 로그 소스, 계정에 저장된 위치 및 액세스할 수 있는 사용자를 이해합니다.
- 조사 중에 CloudWatch Insights를 사용하여 로그를 쿼리하는 방법을 이해합니다.
- 리소스(EC2, IAM, S3, son on)별로 사용할 수 있는 격리 옵션과 격리 시 워크로드 가용성에 미치는 결과를 이해합니다.

감지

AWS 계정을 관리하는 동안 AMS는 Amazon CloudWatch, Amazon GuardDuty, VPC 흐름 로그, Amazon Macie 및 Amazon 내부 위협 인텔리전스 피드를 포함하되 이에 국한되지 않는 탐지 소스 및 제어에서 수집된 데이터를 사용하여 사용자 동작, 계정 활동 AWS Config 및 잠재적 보안 이벤트의 이상을 모니터링합니다.

AMS는 네이티브 AWS 서비스와 기타 탐지 기술을 모두 사용하여 다음에서 생성된 보안 이벤트에 대응합니다.

- Config 적합성 조사 결과 유형
- GuardDuty 결과 유형
- Macie 결과 유형

- Amazon Route 53 Resolver DNS 방화벽 이벤트
- AMS 보안 이벤트(클라우드 감시 경보)

서비스, 제품 및 위협 에코시스템이 발전함에 따라 추가 조사 결과가 추가됩니다.

AMS에 보안 이벤트 보고

AMS 지원 포털 또는 지원 센터를 통해 인시던트를 제기하여 AMS에 보안 인시던트를 알리거나 조사를 요청합니다.

분석

보안 이벤트를 식별하고 보고한 후 다음 단계는 보고된 이벤트가 거짓 긍정인지 실제 인시던트인지 분석하는 것입니다. AMS는 자동화 및 수동 조사 기술을 사용하여 보안 이벤트를 처리합니다. 분석에는 네트워크 트래픽 로그, 호스트 로그, CloudTrail 이벤트, AWS 서비스 로그 등과 같은 다양한 탐지 소스의 로그에 대한 조사가 포함됩니다. 또한이 분석에서는 상관관계를 기준으로 이상 동작을 보여주는 패턴을 찾습니다.

파트너십은 계정 환경과 관련된 컨텍스트를 이해하고 계정 및 워크로드에 일반적인 사항을 설정하는 데 필요합니다. 이를 통해 AMS는 이상을 더 빠르게 식별하고 인시던트 대응을 가속화할 수 있습니다.

보안 이벤트에 대한 AMS의 통신 처리

AMS는 인시던트 티켓을 통해 보안 담당자를 참여시켜 조사 중에 정보를 제공합니다. AMS 클라우드 서비스 제공 관리자(CSDM)와 AMS 클라우드 아키텍트(CA)는 활성 보안 조사 중에 통신을 위해에 문의할 수 있는 담당자입니다.

통신에는 보안 알림이 생성될 때의 자동 알림, 이벤트 분석 후의 통신, 통화 브리지 설정, 로그 파일, 감염된 리소스의 스냅샷, 보안 이벤트 중에 사용자에게 조사 결과 가져오기와 같은 아티팩트의 지속적인 전달이 포함됩니다.

AMS 보안 알림에 포함된 표준 필드는 다음과 같습니다. 이러한 필드는 문제 해결을 위해 조직 내 적절한 팀에 이벤트를 라우팅할 수 있도록 정보를 제공합니다.

- 결과 유형
- 결과 식별자(해당하는 경우)
- 심각도 찾기
- 결과 설명
- 생성된 날짜 및 시간 찾기

- AWS 계정 ID
- 리전(해당하는 경우)
- AWS 리소스(IAM user/role/policy, EC2, S3, EKS)

결과 유형에 따라 추가 필드가 제공됩니다. 예를 들어 EKS 결과에는 포드, 컨테이너 및 클러스터 세부 정보가 포함됩니다.

격리

AMS의 억제 접근 방식은 사용자와의 파트너십입니다. 네트워크 격리, IAM 사용자 또는 역할 프로비저닝 해제, 인스턴스 재구축 등과 같은 억제 활동으로 인해 발생할 수 있는 비즈니스 및 워크로드 영향을 이해합니다.

억제의 필수 부분은 의사 결정입니다. 예를 들어 시스템을 종료하거나, 네트워크에서 리소스를 격리하거나, 액세스 또는 종료 세션을 끕니다. 인시던트를 억제할 사전 결정된 전략과 절차가 있는 경우 이러한 결정을 더 쉽게 내릴 수 있습니다. AMS는 억제 전략을 제공한 다음 억제 작업 구현과 관련된 위험을 고려한 후 솔루션을 구현합니다.

분석 중인 리소스에 따라 다양한 억제 옵션이 있습니다. AMS는 인시던트 조사 중에 여러 유형의 억제가 동시에 배포될 것으로 예상합니다. 이러한 예제 중 일부는 다음과 같습니다.

- 보호 규칙을 적용하여 무단 트래픽 차단(보안 그룹, NACL, WAF 규칙, SCP 규칙, 거부 목록, 격리 또는 차단으로 서명 작업 설정)
- 리소스 격리
- 네트워크 격리
- IAM 사용자, 역할 및 정책 비활성화
- IAM 사용자, 역할 권한 수정/축소
- 컴퓨팅 리소스 종료/일시 중지/삭제
- 영향을 받는 리소스에서 퍼블릭 액세스 제한
- 액세스 키, API 키 및 암호 교체
- 공개된 자격 증명 및 민감한 정보 스캐러빙

AMS는 위험 선호도 내에 있는 각 주요 인시던트 유형에 대한 억제 전략 유형을 고려하는 것이 좋습니다. 인시던트 발생 시 의사 결정에 도움이 되는 기준이 명확하게 문서화되어 있습니다. 적절한 전략을 결정하기 위한 기준은 다음과 같습니다.

- 리소스의 잠재적 손상
- 증거 보존
- 서비스 사용 불가(예: 네트워크 연결, 외부 당사자에게 제공되는 서비스)
- 전략을 구현하는 데 필요한 시간 및 리소스
- 전략의 효율성(예: 부분 격리, 전체 격리)
- 솔루션의 영구성(예: 단방향 출입구와 양방향 출입구 결정)
- 솔루션 기간(예: 긴급 해결 방법은 4시간 내에 제거, 임시 해결 방법은 2주 내에 제거, 영구 솔루션).
- 켤 수 있는 보안 제어를 적용하여 위험을 낮추고 시간을 내어 보다 효과적인 억제를 정의하고 구현할 수 있습니다.

억제 속도가 매우 중요하므로 AMS는 단기 및 장기 접근 방식을 전략화하여 효율적이고 효과적인 억제를 달성하기 위해 단계적 접근 방식을 권장합니다.

이 가이드를 사용하여 리소스 유형에 따라 다양한 기법이 포함된 억제 전략을 고려하세요.

- 억제 전략
 - AMS가 보안 인시던트의 범위를 식별할 수 있습니까?
 - 그렇다면 모든 리소스(사용자, 시스템, 리소스)를 식별합니다.
 - 그렇지 않으면 식별된 리소스에 대해 다음 단계를 실행하는 것과 병행하여 조사합니다.
 - 리소스를 격리할 수 있나요?
 - 그렇다면 영향을 받는 리소스를 격리합니다.
 - 그렇지 않은 경우 시스템 소유자 및 관리자와 협력하여 문제를 격리하는 데 필요한 추가 조치를 결정합니다.
 - 영향을 받는 모든 리소스가 영향을 받지 않는 리소스로부터 격리되어 있나요?
 - 그렇다면 다음 단계로 계속 진행합니다.
 - 그렇지 않은 경우 인시던트가 더 이상 에스컬레이션되지 않도록 단기 격리가 완료될 때까지 영향을 받는 리소스를 계속 격리합니다.
- 시스템 백업
 - 추가 분석을 위해 영향을 받는 시스템의 백업 복사본이 생성되었나요?
 - 포렌식 사본은 암호화되어 안전한 위치에 저장되나요?
 - 그렇다면 다음 단계로 계속 진행합니다.
 - 그렇지 않으면 포렌식 이미지를 암호화한 다음 안전한 위치에 저장하여 우발적인 사용, 손상 및 변조를 방지합니다.

근절

인시던트가 억제된 후 다음 복구 단계로 진행하기 전에 시스템을 보호하기 위해 위협 원인을 완전히 제거하기 위해 근절이 필요할 수 있습니다. 제거 단계에는 멀웨어 삭제 및 손상된 사용자 계정 제거, 악용된 모든 취약성 식별 및 완화가 포함될 수 있습니다. 근절 중에는 환경 내에서 영향을 받는 모든 계정, 리소스 및 인스턴스를 식별하여 문제를 해결하는 것이 중요합니다.

문제 해결 단계가 우선시되도록 단계적 접근 방식으로 근절 및 복구를 수행하는 것이 모범 사례입니다. 대규모 인시던트의 경우 복구에 몇 개월이 걸릴 수 있습니다. 초기 단계의 의도는 향후 인시던트를 방지하기 위해 비교적 빠른(수일에서 수주) 고가치 변경으로 전반적인 보안을 강화하는 것이어야 합니다. 이후 단계에서는 엔터프라이즈를 최대한 안전하게 유지하기 위해 장기 변경(예: 인프라 변경)과 지속적인 작업에 중점을 두어야 합니다.

일부 인시던트의 경우 근절이 필요하지 않거나 복구 중에 수행됩니다.

다음을 고려하세요.

- 시스템을 다시 이미지화한 다음 패치 또는 기타 대응책으로 강화하여 공격 위협을 방지하거나 줄일 수 있습니까?
- 공격자가 남긴 모든 멀웨어 및 기타 아티팩트가 제거되고 영향을 받는 시스템이 추가 공격에 대해 강화되나요?

복구

AMS는 고객과 협력하여 시스템을 정상 작동으로 복원하고, 시스템이 정상적으로 작동하는지 확인하고, (해당하는 경우) 취약성을 해결하여 유사한 인시던트를 방지합니다.

다음을 고려하세요.

- 영향을 받는 시스템(들)이 최근 공격 및 가능한 향후 공격에 대해 패치되고 강화됩니까?
- 영향을 받는 시스템을 다시 프로덕션 환경으로 복원할 수 있는 날짜와 시간은 언제입니까?
- 프로덕션으로 복원하는 시스템이 초기 공격 기법에 취약하지 않은지 테스트, 모니터링 및 확인하는데 사용할 도구는 무엇입니까?

사후 인시던트 보고서

이벤트 후 AMS는 모든 보안 인시던트에 대한 조사 검토 프로세스를 실행합니다. 또한 AMS는 시스템 또는 개선의 여지가 있을 수 있는 절차적 누락으로 인한 보안 인시던트를 해결하기 위해 오류 수정

(COE) 프로세스를 시작합니다. AMS는 고객과 협력하여 보안 조사 경험을 지속적으로 개선합니다. COE 프로세스는 AMS가 고객에게 영향을 미치는 이벤트의 기여 요인을 식별하고 이러한 원인을 유사한 이벤트의 재발을 방지하거나 영향 기간 또는 수준을 완화할 수 있는 다음 작업 항목에 연결하는 데 도움이 됩니다.

보안 인시던트에 대한 조사 검토 프로세스는 개선 기회를 식별하기 위해 다음 항목을 다룹니다.

- 인시던트 시작부터 인시던트 검색, 초기 영향 평가, 인시던트 처리 프로세스의 각 단계(예: 억제, 복구)까지의 경과 시간은 얼마였나요?
- 인시던트 대응 팀이 인시던트의 초기 보고서에 응답하는 데 얼마나 걸렸나요?
- 초기 영향 분석을 수행하는 데 얼마나 걸렸나요?
- 이 문제를 예방할 수 있었고 어떻게 예방할 수 있었나요? 이를 방지할 수 있는 도구나 프로세스가 있나요?
- 이를 더 빨리, 그리고 어떻게 감지할 수 있었을까요?
- 조사 속도를 높일 수 있었던 이유는 무엇입니까?
- 문서화된 인시던트 대응 절차를 따랐습니까? 적절했나요?
- 다른 이해관계자와의 정보 공유가 적시에 이루어졌습니까? 어떻게 개선할 수 있습니까?
- 다른 팀(AWS 보안, 계정 팀, AWS 개발 팀 및 고객 보안 팀)과의 협업이 유효했나요? 그렇지 않다면 개선해야 할 점은 무엇입니까?
- 어떤 준비 단계가 누락되어 있어 도움이 되었을 수 있습니다. 에스컬레이션 매트릭스, RACI, 공동 책임 모델 등이 이에 해당하나요? 런북을 업데이트해야 하나요?
- 초기 영향 평가와 최종 영향 평가의 차이점은 무엇입니까? 인시던트 대응 초기에 평가의 정확도를 높이기 위해 무엇을 할 수 있습니까?
- 학습한 교훈의 작업 항목은 무엇입니까?

AMS의 보안 인시던트 대응 런북

이 섹션에는 두 개의 실행서가 포함되어 있습니다.

- [루트 사용자 활동에 대한 응답](#)
- [맬웨어 이벤트에 대한 응답](#)

루트 사용자 활동에 대한 응답

[루트 사용자는](#) AWS 계정 내의 수퍼유저입니다. AMS는 루트 사용량을 모니터링합니다. 계정 설정을 변경하고, 결제 및 비용 관리에 대한 액세스를 활성화 AWS Identity and Access Management (IAM)하고, 루트 암호를 변경하고, 다중 인증(MFA)을 활성화하는 등 루트 사용자가 필요한 몇 가지 작업에만 루트 사용자를 사용하는 것이 좋습니다. 자세한 내용은 [루트 사용자 자격 증명이 필요한 작업을 참조하세요](#).

AMS에 계획된 루트 사용량을 알리는 방법에 대한 자세한 내용은 [AMS에서 루트 계정을 사용하는 시기](#)와 [방법을 참조하세요](#).

루트 사용자 활동이 감지되면 로그인 시도가 실패하여 로그인 성공 후 계정에서 무차별 대입 공격 또는 활동을 나타낼 수 있으며 이벤트가 생성되고 정의된 보안 연락처로 인시던트가 전송됩니다.

AWS Managed Services Operations는 계획되지 않은 루트 사용자 활동을 조사하고, 데이터 수집, 분류 및 분석을 수행하고, 지시에 따라 억제 활동을 수행한 다음 사후 이벤트 분석을 수행합니다.

AMS Advanced 운영 모델을 사용하는 경우 AMS CSDM 및 AMS Ops 엔지니어로부터 루트 사용자 자격 증명을 보호할 AMS의 책임으로 인해 계획되지 않은 루트 사용자 활동을 확인하는 추가 커뮤니케이션을 받게 됩니다. AMS는 경로를 확인할 때까지 루트 사용자 활동을 조사합니다.

준비

불필요한 인시던트 대응 활동을 방지하기 위해 계획된 이벤트의 데이터 및 시간과 함께 AMS 서비스 요청을 제출하여 계획된 루트 사용자 사용에 대해 AMS에 알립니다.

AMS로 GameDays를 정기적으로 수행하여 AMS의 고객 인시던트 대응 프로세스, 최신 사용자 및 시스템을 검증하고 책임 있는 개인과 함께 메모리를 구축하여 인시던트 대응 속도를 높입니다.

단계 A: 감지

AMS는 GuardDuty 및 AMS 모니터링을 포함한 탐지 소스를 통해 계정의 루트 활동을 모니터링합니다.

AMS Accelerate를 사용하는 경우 운영 모델은 예상치 못한 루트 사용자 활동에 대한 조사를 요청하는 인시던트에 응답합니다. 이 경우 AMS 작업은 손상된 계정 실행서를 시작합니다.

AMS Advanced가 있는 경우 운영 모델은 인시던트에 대응하거나 CSDM에 계획된 루트 사용자 활동을 알려 활성 계정 침해 조사를 종료합니다.

단계 B: 분석

AMS는 활동이 승인되지 않은 것으로 확인되면 루트 사용자 이벤트에 대한 철저한 조사를 수행합니다. 로그와 이벤트는 자동화와 AMS 보안 대응 팀을 모두 사용하여 루트 사용자의 이상 및 예상치 못한 동

작에 대해 분석됩니다. 활동을 알 수 없는지, 권한이 부여된 루트 사용자 이벤트인지 또는 추가 조사가 필요한지 확인하는 데 도움이 되는 로그가 제공됩니다.

내부 검사를 지원하기 위해 조사 중에 제공되는 정보의 몇 가지 예는 다음과 같습니다.

- 계정 정보: 루트 계정이 사용된 계정은 무엇입니까?
- 루트 사용자의 이메일 주소: 각 루트 사용자는 조직의 이메일 주소와 연결됩니다.
- 인증 세부 정보: 루트 사용자는 어디에서 언제 환경에 액세스했습니까?
- 활동 레코드: 루트로 로그인할 때 사용자가 수행한 작업은 무엇입니까? 이러한 레코드는 CloudWatch 이벤트의 형태입니다. 이러한 로그를 읽는 방법을 이해하면 조사에 도움이 됩니다.

분석 정보를 수신하고 조직 내 계정의 승인된 연락 지점에 도달하는 방법을 계획할 준비가 되어 있는 것이 모범 사례입니다. 루트 사용자는 개인으로 이름이 지정되지 않으므로 조직 내 계정에 사용되는 루트 이메일 주소에 액세스할 수 있는 사람을 결정하면 질문을 내부적으로 빠르게 라우팅하는 데 도움이 됩니다.

단계 C: 포함 및 제거

AMS는 보안 팀과 협력하여 승인된 고객 보안 담당자의 지시에 따라 제한을 수행합니다. 억제 옵션은 다음과 같습니다.

- 적절한 자격 증명 및 키 교체.
- 계정 및 리소스에 대한 활성 세션을 종료합니다.
- 생성된 리소스 제거.

억제 활동 중에 AMS는 보안 팀과 긴밀하게 협력하여 워크로드 종단을 최소화하고 루트 자격 증명을 적절하게 보호합니다.

억제 계획이 완료되면 필요에 따라 AMS 운영 팀과 협력하여 복구 작업을 수행합니다.

사후 인시던트 보고서

필요에 따라 AMS는 조사 검토 프로세스를 시작하여 학습한 교훈을 식별합니다. COE 완료의 일환으로 AMS는 영향을 받는 고객에게 관련 조사 결과를 전달하여 인시던트 대응 프로세스를 개선하는 데 도움을 줍니다.

AMS는 조사의 모든 최종 세부 정보를 문서화하고 적절한 지표를 수집한 다음 할당된 CSDM 및 CA를 포함하여 정보가 필요한 모든 AMS 내부 팀에 인시던트를 보고합니다.

맬웨어 이벤트에 대한 응답

Amazon EC2 인스턴스는 조직 내 애플리케이션 팀이 배포한 타사 소프트웨어 및 사용자 지정 개발 소프트웨어를 비롯한 다양한 워크로드를 호스팅하는 데 사용됩니다. AMS는 AMS에서 패치를 적용하고 지속적으로 유지 관리하는 이미지에 워크로드를 배포하도록 권장하고 제공합니다.

인스턴스를 작동하는 동안 AMS는 Amazon GuardDuty, 엔드포인트 보호, 네트워크 트래픽 및 Amazon 내부 위협 인텔리전스 피드를 비롯한 다양한 보안 탐지 제어를 통해 동작 또는 활동의 이상을 모니터링합니다.

AMS Advanced 운영 모델을 사용하는 AMS 고객은 프로비저닝된 리소스에 엔드포인트 보안(EPS) 모니터링 클라이언트를 자동으로 설치합니다. 이렇게 하면 이벤트가 감지될 때 보안 인시던트 생성을 포함하여 리소스가 연중무휴 모니터링되고 지원됩니다.

또한 AMS는 GuardDuty 맬웨어 조사 결과를 모니터링합니다. 활성화된 경우 AMS Advanced와 AMS Accelerate 모두에서 사용할 수 있습니다. 자세한 내용은 [Amazon GuardDuty의 맬웨어 보호](#)를 참조하세요.

Note

[Bring Your Own EPS](#)를 선택한 경우 인시던트 대응 프로세스는이 페이지에 설명된 것과 다릅니다. 자세한 내용은 참조된 설명서를 참조하세요.

맬웨어가 감지되면 인시던트가 생성되고 이벤트에 대한 알림을 받게 됩니다. 이 알림 뒤에는 해결 활동이 발생합니다. AMS Operations는 데이터 수집, 분류 및 분석을 조사하고 수행한 다음 사용자의 지시에 따라 억제 활동을 수행한 다음 사후 이벤트 분석을 수행합니다.

단계 A: 감지

AMS는 GuardDuty 및 엔드포인트 보안 솔루션 모니터링을 사용하여 인스턴스의 이벤트를 모니터링합니다. AMS는 조사 결과 또는 알림 유형에 따라 억제 또는 위험 수용 결정을 내리는 데 도움이 되는 적절한 보강 및 분류 활동을 결정합니다.

데이터 수집은 결과 유형에 따라 수행됩니다. 데이터 수집에는 영향을 받는 계정 내부 및 외부에서 여러 데이터 소스를 쿼리하여 관찰된 활동 또는 우려되는 구성에 대한 그림을 작성하는 작업이 포함됩니다.

AMS는 영향을 받는 계정 또는 AMS 위협 인텔리전스 플랫폼의 다른 경보 및 알림 또는 원격 측정과 결과의 상관 관계를 수행합니다.

단계 B: 분석

데이터가 수집되면 데이터를 분석하여 우려되는 활동 또는 지표를 식별합니다. 조사의이 단계에서 AMS는 고객과 협력하여 인스턴스 및 워크로드에 대한 비즈니스 및 도메인 지식을 통합하여 무엇이 예상되고 무엇이 일반적이지 않은지 이해하는 데 도움을 줍니다.

내부 검사를 지원하기 위해 조사 중에 제공되는 정보의 몇 가지 예는 다음과 같습니다.

- 계정 정보: 맬웨어 활동이 관찰된 계정은 무엇입니까?
- 인스턴스 세부 정보: 맬웨어 이벤트와 관련된 인스턴스(들)는 무엇입니까?
- 이벤트 타임스탬프: 알림이 언제 트리거되었습니까?
- 워크로드 정보: 인스턴스에서 실행 중인 것은 무엇입니까?
- 해당하는 경우 맬웨어 세부 정보: 맬웨어 패밀리 및 맬웨어에 대한 오픈 소스 정보.
- 사용자 또는 역할 세부 정보: 활동의 영향을 받고 활동에 관여한 사용자 또는 역할은 무엇입니까?
- 활동 레코드: 인스턴스에 기록되는 활동은 무엇입니까? 이는 CloudWatch 이벤트 및 인스턴스의 시스템 이벤트의 형태입니다. 이러한 로그를 읽는 방법을 이해하면 조사에 도움이 됩니다.
- 네트워크 활동: 인스턴스에 연결하는 엔드포인트, 인스턴스가 연결하는 엔드포인트, 트래픽 분석이란 무엇입니까?

조사 정보를 수신하고 조직 내 계정, 인스턴스 및 워크로드의 적절한 연락 지점에 연락하는 방법에 대한 계획을 세우는 것이 모범 사례입니다. 네트워크 토폴로지와 예상 연결을 이해하면 영향 분석을 가속화하는 데 도움이 될 수 있습니다. 환경에서 계획된 침투 테스트와 애플리케이션 소유자가 수행한 최근 배포에 대한 지식도 조사 속도를 높일 수 있습니다.

활동이 계획되고 승인되었다고 판단되면 인시던트가 업데이트되고 조사가 종료됩니다. 손상이 확인되면 사용자와 AMS가 적절한 억제 계획을 결정합니다.

속도 C: 포함 및 제거

AMS는 고객과 협력하여 수집된 데이터와 알려진 정보를 기반으로 적절한 억제 활동을 결정합니다. 억제 옵션은 다음을 포함하지만 이에 국한되지는 않습니다.

- 스냅샷을 통한 데이터 보존
- 인스턴스 내부 또는 외부의 트래픽을 제한하도록 네트워크 규칙 수정
- SCP, IAM 사용자 및 역할 정책을 수정하여 액세스 제한
- 인스턴스 종료, 일시 중지 또는 끄기
- 영구 연결 종료

- 적절한 자격 증명/키 교체

인스턴스에 대해 근절 활동을 수행하도록 선택하면 AMS가 이를 달성할 수 있도록 지원합니다. 옵션은 다음을 포함하지만 이에 국한되지는 않습니다.

- 원치 않는 소프트웨어 제거
- 완전히 패치된 깨끗한 이미지에서 인스턴스 재구축 및 애플리케이션 및 구성 재배포
- 이전 백업에서 인스턴스 복원
- 워크로드를 호스팅하는 데 적합할 수 있는 계정 내 다른 인스턴스에 애플리케이션 및 서비스를 배포합니다.

서비스를 복원하기 전에 인스턴스에서 맬웨어가 전달되고 실행되는 방법을 결정하여 인스턴스에서 맬웨어가 다시 발생하지 않도록 추가 제어가 적용되는지 확인하는 것이 중요합니다. AMS는 포렌식을 지원하는 데 필요한 추가 인사이트 또는 정보를 포렌식 파트너 또는 팀에 제공합니다.

이 시점에서 복구 활동을 위해 AMS Operations와 협력합니다. AMS는 사용자와 긴밀하게 협력하여 워크로드 중단을 최소화하고 인스턴스를 보호합니다.

사후 인시던트 보고서

필요에 따라 AMS는 조사 검토 프로세스를 시작하여 학습한 교훈을 식별합니다. COE 완료의 일환으로 AMS는 인시던트 대응 프로세스를 개선하는 데 도움이 되도록 관련 조사 결과를 사용자에게 전달합니다.

AMS는 조사의 최종 세부 정보를 문서화하고, 적절한 지표를 수집하고, 할당된 CSDM 및 CA를 포함하여 정보가 필요한 AMS 내부 팀에 인시던트를 보고합니다.

AMS Advanced의 변경 요청 보안 검토

AWS Managed Services 변경 요청 검토 프로세스는 AMS가 요청된 변경 사항이 계정에서 사용자를 대신하여 구현될 때 보안 검토를 수행하도록 합니다.

[AMS Advanced 기술 표준](#) 최소 보안 기준, 구성 및 프로세스를 정의하여 계정의 기본 보안을 설정합니다. AMS가 요청된 변경 사항을 구현하면 이러한 표준을 따릅니다.

AMS는 AMS 기술 표준을 기준으로 모든 변경 요청을 평가합니다. 기술 표준을 벗어나 계정의 보안 태세를 저하시킬 수 있는 모든 변경 사항은 보안 검토 프로세스를 거칩니다. 이 프로세스 중에 AMS에서 관련 위험을 강조 표시하고 승인된 위험 승인자가 검토 및 승인하여 보안 및 비즈니스 요구 사항의 균형을 유지합니다.

고객 보안 위험 관리 프로세스

AMS Advanced Customer Security Risk Management(CSRM) 프로세스는 위험을 명확하게 식별하고 적절한 소유자에게 알리는 데 도움이 됩니다. 이 프로세스는 환경의 보안 위험을 최소화하고 식별된 위험에 대한 지속적인 운영 오버헤드를 줄입니다.

기본적으로 조직의 누군가가 AMS가 관리형 환경에 대한 변경을 구현하도록 요청하면 AMS는 변경 사항을 검토하여 요청이 기술 표준을 벗어나 계정의 보안 태세를 변경할 수 있는지 확인합니다. 보안 위험이 높거나 매우 높은 경우 권한 있는 보안 담당자가 변경 검토를 수락하거나 거부합니다. 요청된 변경 사항도 AMS의 계정 운영 능력에 부정적인 영향을 미치는지 평가됩니다. 검토에서 가능한 부정적인 영향이 발견되면 AMS 내에서 추가 검토 및 승인이 필요합니다.

위험이 높거나 매우 높은 경우 CSRM 프로세스의 승인 기반 워크플로에서 옵트아웃할 수 있습니다. 특정 계정의 CSRM 옵션을 표준 CSRM에서 알림 전용으로 변경하려면 Cloud Service Delivery Manager와 협력하여 일회성 위험 수락을 생성합니다. 알림 전용 옵션을 선택하면 AMS는 위험 범주에 관계없이 요청된 변경 사항을 구현합니다. 또한 AMS는 변경 구현 전에 승인을 구하는 대신 승인된 위험 승인자에게 위험 알림을 보냅니다. AMS CSRM 프로세스, 새 AMS 계정을 온보딩할 때 기본 CSRM 옵션을 변경하는 방법 또는 기존 계정을 업데이트하는 방법에 대한 자세한 내용은 Cloud Architects 또는 Cloud Service Delivery Manager에게 문의하세요.

Note

AMS는 모든 계정에서 표준 CSRM의 기본 옵션을 사용할 것을 적극 권장합니다.

AMS Advanced 기술 표준

다음은 AMS Advanced 기술 표준 범주입니다.

ID	범주
AMS-STD-001	태그 지정 구성
AMS-STD-002	AWS Identity and Access Management
AMS-STD-003	네트워크 보안
AMS-STD-004	침투 테스트

ID	범주
AMS-STD-005	Amazon GuardDuty
AMS-STD-006	호스트 보안
AMS-STD-007	로깅
AMS-STD-008	AMS-MAD
AMS-STD-009	기타사항

AMS Advanced의 표준 제어

다음은 AMS의 표준 컨트롤입니다.

AMS-STD-001 - 태그 지정 구성

다음은 001 - 태그 지정 구성에 대한 표준 컨트롤입니다.

1. 운영 및 관리를 위해 AMS 팀에 필요한 모든 AWS 리소스에는 다음과 같은 키-값 페어가 있어야 합니다.
 - AppId= AMSInfrastructure
 - 환경= AMSInfrastructure
 - AppName = AMSInfrastructure
 - AMSResource=True
2. 이전에 나열된 태그 이외의 AMS 팀에 필요한 모든 태그에는 AMS 접두사 목록에 언급된 접두사가 있어야 합니다(참고 참조).
3. AMS 팀(AppId, 환경 및 AppName)에 필요한 태그 값은 변경 요청에 따라 사용자가 생성한 모든 리소스에서 변경할 수 있습니다.
4. AMS에 필요한 스택의 태그는 변경 요청에 따라 삭제해서는 안 됩니다.
5. 2번에서 언급한 것처럼 인프라에 AMS 태그 이름 지정 규칙을 사용할 수 없습니다.
6. AMS에 필요한 리소스에서 사용자 지정 태그를 생성할 수 있습니다(일반적으로 결제 및 비용 보고 사용 사례의 경우). 사용자 지정 태그는 템플릿 업데이트가 아닌 스택 업데이트로 리소스를 업데이트하는 경우 유지됩니다.

 Note

AMS 접두사 목록

1. ams-*
2. AWSManagedServices*
3. /ams/*
4. ams*
5. AMS*
6. Ams*
7. mc*
8. MC*
9. 맥*
- 10.sentinel*
- 11.Sentinel*
- 12.Managed_Services*
- 13.NewAMS*
- 14.AWS_*
- 15.aws*
- 16.VPC_*
- 17.CloudTrail*
- 18.Cloudtrail*
- 19/aws_reserved/
- 20.수 집*
- 21.EPSDB*
- 22.MMS*
- 23.TemplateId*
- 24.StackSet-ams*
- 25.StackSet-AWS-Landing-Zone
- 26.IAMPolicy*
- 27.고객-mc-*

- 28.루트*
- 29.LandingZone*
- 30.StateMachine*
- 31.codedeploy_service_role
- 32.관리 호스트
- 33.sentinel.int.
- 34.eps
- 35.UnhealthyInServiceBastion
- 36.ms-

AMS-STD-002 - AWS Identity and Access Management (IAM)

ID	기술 표준
1.0	제한 시간 지속 시간
1.1	페더레이션 사용자 기본 제한 시간 세션은 1시간이며 최대 4시간까지 늘릴 수 있습니다.
1.2	기본 스택 액세스 시간은 12시간입니다.
2.0	AWS 루트 계정 사용
2.1	어떤 이유로든 루트 계정 사용량이 있는 경우 관련 조사 결과를 생성하도록 Amazon GuardDuty를 구성해야 합니다.
2.2	단일 계정 랜딩 존(SALZ) 계정 및 다중 계정 랜딩 존(MALZ) 관리 계정(이전에는 마스터/청구 계정이라고 함)의 경우, 루트 사용자 계정에 가상 MFA가 활성화되어 있어야 하며 계정 온보딩 중에 MFA 소프트 토큰이 삭제되어 AMS와 고객 모두 루트로 로그인할 수 없습니다. AMS Cloud Service Delivery Manager(CSDM)와 함께 표준 AWS 루트 암호 분실 프로세스를 따라야 합니다.

ID	기술 표준
	다. 이 구성은 AMS 관리형 계정의 수명 주기 동안 유지되어야 합니다.
2.3	루트 계정에 대한 액세스 키를 생성해서는 안 됩니다.
3.0	사용자 생성 및 수정
3.1	프로그래밍 방식 액세스 권한과 읽기 전용 권한이 있는 IAM 사용자/역할은 시간 제한 정책 없이 생성할 수 있습니다. 그러나 계정의 모든 Amazon Simple Storage Service 버킷에서 객체(예: S3:GetObject)를 읽을 수 있는 권한은 허용되지 않습니다.
3.1.1	콘솔 액세스 및 읽기 전용 권한을 가진 IAM 인간 사용자는 시간 제한 정책(최대 180일)을 사용하여 생성할 수 있지만 시간 제한 정책을 removal/renewal/extension하면 위험 알림이 발생합니다. 그러나 계정의 모든 S3 버킷에서 객체(예: S3:GetObject)를 읽을 수 있는 권한은 허용되지 않습니다.
3.2	고객 계정의 인프라 변경 권한(쓰기 및 권한 관리)을 사용한 콘솔 및 프로그래밍 방식 액세스에 대한 IAM 사용자 및 역할은 위험 수락 없이 생성해서는 안 됩니다. 특정 버킷이 비 AMS 관련 태그의 범위 및 태그 지정 작업에 있는 한 위험 수락 없이 허용되는 S3 객체 수준 쓰기 권한에는 예외가 있습니다.

ID	기술 표준
3.3	SALZ 또는 MALZ 애플리케이션 계정 <code>customer_servicenow_user</code> 및 *코어 계정*의 ServiceNow 통합에 이름이 지정되고 <code>customer_servicenow_logging_user</code> 필요한 프로그래밍 방식 액세스 권한이 있는 IAM 사용자는 시간 제한 정책 없이 생성할 수 있습니다.
3.4	SALZ <code>customer_cloud_endure_policy</code> 및 MALZ 계정에서 CloudEndure 통합에 필요한 및 <code>customer_cloud_endure_deny_policy</code> (읽기 전용 액세스 포함)를 사용하고 프로그래밍 방식으로 액세스할 수 있는 IAM 사용자는 생성할 수 있지만 계획된 마이그레이션 기간 동안 시간 제한 정책이 필요합니다. 시간 제한은 RA 없이 최대 180일일 수 있습니다. 또한 SCP는 이러한 정책이 필요한 기간 동안 작동하도록 MALZ 계정에 대한 변경 권한이 부여됩니다. 필요에 따라 적절한 마이그레이션 기간을 정의하고 필요에 따라 조정합니다.
4.0	정책, 작업 및 APIs
4.1	SALZ 계정의 모든 IAM 사용자 및 역할에는 AMS 인프라가 실수로 또는 의도적으로 손상되지 않도록 보호하기 위한 기본 고객 거부 정책 (CDP)이 연결되어 있어야 합니다.
4.2	AMS SCPs MALZ의 모든 AMS 관리 계정에서 활성화되어야 합니다.
4.3	<code>PutKeyPolicy</code> 및와 같이 KMS 키에 대한 관리 작업을 수행할 수 있는 자격 증명은 AMS 연산자 및 자동화 보안 주체로만 제한되어야 <code>ScheduleKeyDeletion</code> 합니다.

ID	기술 표준
4.4	정책은 위험 수락 없이 "Effect": "Allow" with "Action": "*" over "Resource": "*"에 해당하는 문과 함께 관리자 액세스 권한을 제공해서는 안 됩니다.
4.5	IAM 정책에는 위험 수락 없이 버킷에서 S3:*** 허용 작업이 포함된 작업이 포함되어서는 안 됩니다.
4.6	고객 IAM 정책의 AMS 인프라 키에 대한 KMS 키 정책에 대한 API 호출은 허용되지 않아야 합니다.
4.7	인스턴스 시작 또는 중지, S3 버킷 또는 RDS 인스턴스 생성 등과 같이 변경 관리 프로세스 (RFC)를 우회하는 작업은 허용되지 않아야 합니다.
4.8	Amazon Route 53에서 AMS 인프라 DNS 레코드를 변경하는 작업은 허용되지 않아야 합니다.
4.9	적절한 프로세스를 따른 후 콘솔 액세스 권한이 생성된 IAM 인간 사용자는 신뢰 정책, 역할 수임 및 시간 제한 정책을 제외하고 직접 연결된 정책이 없어야 합니다.
4.10	동일한 계정 AWS Secrets Manager 내의 특정 보안 암호 또는 네임스페이스에 대한 읽기 액세스 권한이 있는 Amazon EC2 인스턴스 프로파일을 생성할 수 있습니다.
4.11	AWS Managed Services Change Management(AMSCM) 또는 AWS Managed Services Service Knowledge Management System(AMSSKMS) 권한을 모든 역할에 추가할 수 있습니다(SR/Incident/RFC를 열 수 있음).

ID	기술 표준
4.12	IAM 정책에는 AMS Amazon CloudWatch 로그 그룹에서 로그>DeleteLogGroup 및 로그>Delete LogStream 허용 작업이 포함된 작업이 포함되어서는 안 됩니다.
4.13	다중 리전 키를 생성할 수 있는 권한은 허용되지 않아야 합니다.
4.14	계정에 아직 생성되지 않은 S3 버킷 ARNs에 대한 액세스를 제공하려면 서비스별 S3 조건 키를 사용하여 계정 번호를 s3:ResourceAccount 지정합니다.
4.15	사용자 지정 대시보드에 대한 액세스 권한은 확인, 생성, 나열 및 삭제할 수 있지만 Amazon CloudWatch 대시보드에서는 액세스 권한만 보고 나열할 수 있습니다.
4.15.1	S3 스토리지 렌즈 사용자 지정 대시보드에 대한 보기, 생성, 나열 및 삭제 액세스 권한을 가질 수 있습니다.
4.16	Amazon Redshift 데이터베이스에서 작업할 수 있도록 역할/사용자에게 SQL Workbench 관련 전체 권한을 부여할 수 있습니다.
4.17	CLI의 대안으로 고객 역할에 모든 AWS CloudShell 권한을 부여할 수 있습니다.
4.18	가 신뢰할 수 있는 보안 주체 AWS 서비스 인 IAM 역할도 IAM 기술 표준을 준수해야 합니다.
4.19	서비스 연결 역할(SLRs)은 IAM 서비스 팀에서 구축 및 유지 관리하므로 AMS IAM 기술 표준의 적용을 받지 않습니다.

ID	기술 표준
4.20	IAM 정책은 계정의 모든 버킷에서 Amazon S3 버킷 객체(예: Amazon S3:GetObject)에 대한 무제한 읽기 액세스를 허용해서는 안 됩니다. - 개발자 모드 계정에서: 위반하면 위험 알림이 발생합니다. - 개발자가 아닌 모드 계정: 위반 시 위험 수락 필요
4.21	리소스 유형 "savingsplan"에 대한 모든 IAM 권한을 고객에게 부여할 수 있습니다.
4.22	AMS 엔지니어는 Amazon S3, Amazon S3 객체, 데이터베이스)를 수동으로 복사하거나 이동할 수 없습니다. Amazon Relational Database Service DynamoDB
4.23	AMS 관리형 계정에서 추가 액세스를 허용하도록 SCP 정책을 수정해서는 안 됩니다.
4.24	AMS 인프라 또는 관리 기능을 손상시킬 수 있는 SCP 정책 변경은 허용되지 않습니다. (참고: AMS 리소스에는 태그가 AppId= AMSInfrastructure 있으며 AMS 보호 네임스페이스를 따릅니다).
4.25	AMS 자동 IAM 프로비저닝 기능은 계정에서 옵트인 기능으로 활성화해야 합니다.
4.26	AMS 사람이 맡은 역할 또는 사용자는 S3, RDS, DynamoDB, Redshift, ElastiCache, EFS 및 FSx의 고객 콘텐츠에 액세스할 수 없어야 합니다. 또한 고객 콘텐츠에 대한 액세스 권한을 AWS 서비스 부여하는 다른에서 릴리스한 알려진 새 APIs에 대한 액세스는 운영자 역할에서 명시적으로 거부되어야 합니다.

ID	기술 표준
5.0	연동
5.1	인증은 AMS 관리형 계정의 페더레이션을 사용하여 구성해야 합니다.
5.2	AMS AD에서 활성 디렉터리로의 단방향 발신 신뢰만 있어야 합니다(AMS AD는 온프레미스 AD를 신뢰함).
5.3	AMS에 인증하는 데 사용되는 자격 증명 스토어가 AMS 관리형 애플리케이션 계정에 없어야 합니다.
6.0	교차 계정 정책
6.1	IAM 역할은 고객 레코드에 따라 동일한 고객에게 속한 AMS 계정 간에 정책을 신뢰합니다.
6.2	IAM 역할은 AMS와 비 AMS 계정 간의 신뢰 정책을 동일한 AMS 고객이 비 AMS 계정을 소유한 경우에만(동일한 계정인지 확인하거나 이메일 도메인을 고객의 회사 이름과 AWS Organizations 일치시켜) 구성해야 합니다.
6.3	IAM 역할은 위험 수락 없이 AMS 계정과 타사 계정 간의 정책을 신뢰합니다.
6.4	동일한 고객의 AMS 계정 간에 고객 관리형 CMKs에 액세스하는 교차 계정 정책을 구성할 수 있습니다.
6.5	AMS 계정을 통해 비 AMS 계정 내의 모든 KMS 키에 액세스하기 위한 교차 계정 정책을 구성할 수 있습니다.

ID	기술 표준
6.6	타사 계정이 AMS 계정 내의 KMS 키에 액세스하기 위한 교차 계정 정책은 위험 수락 없이 허용되지 않아야 합니다.
6.6.1	비 AMS 계정에서 AMS 계정 내의 모든 KMS 키에 액세스하기 위한 교차 계정 정책은 동일한 AMS 고객이 비 AMS 계정을 소유한 경우에만 구성할 수 있습니다.
6.7	동일한 고객의 AMS 계정 간에 데이터를 저장할 수 있는 모든 S3 버킷 데이터 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 교차 계정 정책을 구성할 수 있습니다.
6.8	읽기 전용 액세스 권한이 있는 AMS 계정의 비 AMS 계정에 데이터를 저장할 수 있는 모든 S3 버킷 데이터 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 교차 계정 정책을 구성할 수 있습니다.
6.9	AMS에서 비 AMS 계정(또는 비 AMS에서 AMS 계정)에 대한 쓰기 권한으로 데이터를 저장할 수 있는 S3 버킷 데이터 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 교차 계정 정책은 동일한 AMS 고객이 비 AMS 계정을 소유한 경우에만(동일 AWS Organizations 한 계정에 있는지 확인하거나 이메일 도메인을 고객의 회사 이름과 일치시켜) 구성해야 합니다.

ID	기술 표준
6.10	읽기 전용 액세스 권한이 있는 AMS 계정의 타사 계정에 데이터를 저장할 수 있는 모든 S3 버킷 데이터 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 교차 계정 정책을 구성할 수 있습니다.
6.11	쓰기 액세스 권한이 있는 AMS 계정의 타사 계정에 데이터를 저장할 수 있는 S3 버킷 데이터 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 교차 계정 정책은 구성하면 안 됩니다.
6.12	데이터를 저장할 수 있는 AMS 고객 S3 버킷 또는 리소스(asAmazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 타사 계정의 교차 계정 정책은 위험 수락 없이 구성해서는 안 됩니다.
7.0	사용자 그룹
7.1	읽기 전용 및 비변동 권한이 있는 IAM 그룹은 허용됩니다.
8.0	리소스 기반 정책
8.1	AMS 인프라 리소스는 리소스 기반 정책을 연결하여 승인되지 않은 자격 증명으로 관리로부터 보호해야 합니다.
8.2	다른 정책을 명시적으로 지정하지 않는 한 리소스는 최소 권한 리소스 기반 정책으로 구성해야 합니다.
9.0	셀프 서비스 프로비저닝된 서비스(SSPS)

ID	기술 표준
9.1	AMS 기본 IAM 역할 또는 정책(인스턴스 프로파일, SSPS, 패턴 포함)은 위험 수락 여부에 관계 없이 수정해서는 안 됩니다. 신뢰 정책에는 예외가 허용됩니다(위험 수락 없음). 역할, 정책 또는 사용자 변경 사항의 태그 지정은 기본 SSP 역할에서도 허용됩니다.
9.3	Systems Manager Automation 콘솔 역할에 대한 SSPS 정책은 기본 역할 이외의 사용자 지정 역할에 연결할 수 없습니다. 다른 SSPS 정책은 정책을 사용자 지정 역할에 연결하는 것이 기본 SSPS 서비스에 대해 의도된 설계 이외의 추가 권한을 제공하지 않는지 확인한 후에만 사용자 지정 IAM 역할에 연결해야 합니다.

AMS-STD-003 - 네트워크 보안

다음은 003 - 네트워크 보안에 대한 표준 제어입니다.

ID	기술 표준
	네트워킹
1.0	모든 EC2 인스턴스는 접속 호스트, 접속 호스트 VPC CIDR 범위 또는 동일한 인스턴스 VPC CIDR 범위를 통해서만 SSH 또는 RDP를 통해 액세스해야 합니다.
2.0	EC2 인스턴스에서 탄력적 IP 허용
3.0	데이터 영역 TLS 1.2 이상에서 AMS 컨트롤 플레인 및 확장별을 사용해야 합니다.
4.0	모든 송신 트래픽은 계정 IGW 또는 TGW를 사용하여 전달해야 합니다.

ID	기술 표준
5.0	9.0에 따라 로드 밸런서에 연결되지 않은 경우 보안 그룹에 인바운드 규칙에서 소스가 0.0.0.0/0이 아니어야 합니다.
6.0	위험 수락 없이 S3 버킷 또는 객체를 공개해서는 안 됩니다.
7.0	포트 SSH/22 또는 SSH/2222(SFTP/2222 아님), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 또는 1604, LDAP/389 또는 636 및 RPC/135에서 서버 관리 액세스는 보안 그룹을 통해 VPC 외부에서 허용되지 않아야 합니다.
8.0	포트(MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433) 또는 사용자 지정 포트의 데이터베이스 관리 액세스는 보안 그룹을 통해 DX, VPC 피어 또는 VPN을 통해 VPC로 라우팅되지 않은 퍼블릭 IPs에서 허용되지 않아야 합니다.
8.1	고객 데이터를 저장할 수 있는 리소스는 퍼블릭 인터넷에 직접 노출되어서는 안 됩니다.
9.0	인터넷에서 포트 HTTP/80, HTTPS/8443 및 HTTPS/443을 통한 직접 애플리케이션 액세스는 로드 밸런서에만 허용되며 EC2 인스턴스, ECS/EKS/Fargate 컨테이너 등과 같은 컴퓨팅 리소스에는 직접 액세스할 수 없습니다.
10.0	고객 프라이빗 IP 범위에서 포트 HTTP/80 및 HTTPS/443을 통한 애플리케이션 액세스를 허용할 수 있습니다.

ID	기술 표준
11.0	AMS 인프라에 대한 액세스를 제어하는 보안 그룹에 대한 모든 변경은 위험 수락 없이 허용되지 않아야 합니다.
12.0	AMS 보안은 보안 그룹이 인스턴스에 연결되도록 요청될 때마다 표준을 나타냅니다.
13.0	포트 3389 및 22의 고객 접속 액세스는 DX, VPC-peer 또는 VPN을 통해 VPC로 라우팅되는 프라이빗 IP 범위에서만 허용되어야 합니다.
14.0	AMS에서 비 AMS 계정(또는 비 AMS에서 AMS 계정)으로의 VPCs와 프라이빗 호스팅 영역의 교차 계정 연결은 내부 도구를 사용하여 동일한 AMS 고객이 비 AMS 계정을 소유한 경우에만 (동일한 AWS 조직 계정인지 확인하거나 이메일 도메인을 고객의 회사 이름과 일치시켜) 구성해야 합니다.
15.0	동일한 고객에게 속한 계정 간의 VPC 피어링 연결을 허용할 수 있습니다.
16.0	AMS 기본 AMIs는 내부 도구를 사용하여 두 계정이 모두 동일한 고객이 소유하는 한(동일한 계정에 있는지 확인하거나 이메일 도메인을 고객의 회사 이름과 일치시켜) 비 AMS AWS Organizations 계정과 공유할 수 있습니다.
17.0	FTP 포트 21은 위험 수락 없이 보안 그룹에 구성해서는 안 됩니다.
18.0	고객이 모든 계정을 소유하는 한 전송 게이트웨이를 통한 교차 계정 네트워크 연결이 허용됩니다.
19.0	프라이빗 서브넷을 퍼블릭으로 설정하는 것은 허용되지 않습니다.

ID	기술 표준
20.0	타사 계정(고객이 소유하지 않음)과의 VPC 피어링 연결은 허용되지 않습니다.
21.0	타사 계정(고객이 소유하지 않음)과의 Transit Gateway 연결은 허용되지 않습니다.
22.0	AMS가 고객에게 서비스를 제공하는 데 필요한 네트워크 트래픽은 고객 네트워크 송신 지점에서 차단되어서는 안 됩니다.
23.0	위험 알림을 통해 동일한 고객이 AWS 계정 소유한와 해석기 규칙을 공유할 수 있습니다.
19.0	ICMP
19.1	고객 인프라에서 Amazon EC2로 인바운드 ICMP를 요청하려면 위험 알림이 필요합니다.
19.2	보안 그룹을 통해 DX, VPC 피어 또는 VPN을 통해 Amazon VPC로 라우팅된 퍼블릭 IPs의 인바운드 요청은 허용됩니다.
19.3	보안 그룹을 통해 DX, VPC-peer 또는 VPN을 통해 Amazon VPC로 라우팅되지 않은 퍼블릭 IPs의 인바운드 요청은 위험 승인을 받아야 합니다.
19.4	Amazon EC2에서 모든 대상으로의 아웃바운드 ICMP 요청이 허용됩니다.
20.0	보안 그룹 공유
20.1	보안 그룹이이 보안 표준을 충족하는 경우 동일한 계정VPCs와 동일한 조직의 계정 간에 공유할 수 있습니다.

ID	기술 표준
20.2	보안 그룹이이 표준을 충족하지 않고 이전에이 보안 그룹에 대해 위험 수락이 필요한 경우, 동일한 계정의 VPCs 간 또는 동일한 조직의 계정 간 보안 그룹 공유 기능의 사용은 해당 VPC 또는 계정에 대한 위험 수락 없이 허용되지 않습니다.

AMS-STD-004 - 침투 테스트

다음은 004 - 침투 테스트를 위한 표준 컨트롤입니다.

1. AMS는 pentest 인프라를 지원하지 않습니다. 이는 고객의 책임입니다. 예를 들어 Kali는 Linux의 AMS 지원 배포판이 아닙니다.
2. 고객은 [침투 테스트](#)를 준수해야 합니다.
3. 고객이 계정 내에서 인프라 침투 테스트를 수행하려는 경우 24시간 전에 AMS에 미리 알려야 합니다.
4. AMS는 고객의 변경 요청 또는 서비스 요청에 명시적으로 명시된 고객 요구 사항에 따라 고객 검사 인프라를 프로비저닝합니다.
5. 인프라를 테스트하는 고객의 자격 증명 관리는 고객의 책임입니다.

AMS-STD-005 - GuardDuty

다음은 005 - GuardDuty의 표준 컨트롤입니다.

1. GuardDuty는 모든 고객 계정에서 항상 활성화되어야 합니다.
2. MALZ의 고객 관리형 애플리케이션 계정(CMA)의 GuardDuty 결과는 운영 팀에 경보를 발생시키지 않습니다.
3. GuardDuty 알림은 동일한 계정 또는 동일한 조직의 다른 관리형 계정 내에 저장되어야 합니다.
4. GuardDuty의 신뢰할 수 있는 IP 목록 기능은 사용해서는 안 됩니다. 대신 자동 보관을 대안으로 사용할 수 있으며, 이는 감사 목적에 유용합니다.
5. 위임된 관리자는 위험 수락 없이 다른 계정에서 GuardDuty를 비활성화하는 등의 높은 권한 작업을 수행할 수 있으므로 MALZ에서 GuardDuty 관리자 위임을 활성화해서는 안 됩니다.

6. GuardDuty Auto Archive Filters는 최대 반환을 위해 최소 범위를 사용해야 합니다. 예를 들어 AMS가 여러 CIDR 블록에서 예측할 수 없는 IPs 여러 개 볼 수 있고 사용하기에 적합한 기업 ASN이 있는 경우 ASN을 사용합니다. 그러나 특정 범위 또는 /32 주소로 범위를 좁힐 수 있는 경우 해당 범위로 범위를 지정합니다.

AMS-STD-006 - 호스트 보안

다음은 006 - 호스트 보안에 대한 표준 제어입니다.

- 바이러스 백신 에이전트는 항상 모든 EC2 인스턴스에서 실행되어야 합니다(예: Trend Micro").
- 맬웨어 방지 모듈을 활성화해야 합니다.
- EPS 에이전트에는 스캔을 위한 모든 디렉터리와 파일이 포함되어야 합니다.
- 바이러스 백신 솔루션으로 격리된 파일은 온디맨드 방식으로와 공유할 수 있습니다.
- 타사 엔드포인트 보안 솔루션을 설치해서는 안 됩니다.
- 바이러스 백신 서명 업데이트 빈도는 하루에 한 번 이상으로 설정해야 합니다.
- 예약된 스캔 빈도는 한 달에 한 번 이상으로 설정해야 합니다.
- 실시간(액세스 중) 스캔은 항상 활성화되고 실행되어야 합니다.
- AMS는 인스턴스에서 AMS가 소유하거나 작성하지 않은 사용자 지정 스크립트를 실행해서는 안 됩니다. (참고: 스택 관리자 액세스 CT를 통해 스택 관리자 액세스를 사용하거나 [AWS Systems Manager 자동화\(AMS SSPS\)](#)를 사용하여 작업을 수행할 수 있습니다.
- Windows 호스트에서 네트워크 수준 인증(NLA)을 비활성화해서는 안 됩니다.
- 호스트 운영 체제는 구성된 패치 주기에 따라 최신 보안 패치를 사용하여 최신 상태여야 합니다.
- AMS 관리형 계정에는 계정에 비관리형 인스턴스가 없어야 합니다.
- AMS에서 인스턴스에 로컬 관리자 계정을 생성할 수 없습니다.
- EC2의 키 페어를 생성해서는 안 됩니다.
- 수명 종료(EOL)로 선언된 운영 체제를 사용해서는 안 되며 공급업체 또는 타사에서 제공하는 추가 보안 지원이 없어야 합니다.

AMS-STD-007 - 로깅

다음은 007 - 로깅에 대한 표준 컨트롤입니다.

ID	기술 표준
1.0	로그 유형
1.1	OS 로그: 모든 호스트는 최소 호스트 인증 이벤트, 승격된 권한의 모든 사용에 대한 액세스 이벤트, 성공 및 실패를 포함한 액세스 및 권한 구성에 대한 모든 변경 사항에 대한 액세스 이벤트를 로깅해야 합니다.
1.2	AWS CloudTrail: 로그를 S3 버킷에 전달하도록 CloudTrail 관리 이벤트 로깅을 활성화하고 구성해야 합니다.
1.3	VPC 흐름 로그: 모든 네트워크 트래픽 로그는 VPC 흐름 로그를 통해 로깅되어야 합니다.
1.4	Amazon S3 서버 액세스 로깅: 로그를 저장하는 AMS 필수 S3 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다.
1.5	AWS Config 스냅샷: AWS Config 모든 리전에서 지원되는 모든 리소스에 대한 구성 변경을 기록하고 구성 스냅샷 파일을 하루에 한 번 이상 S3 버킷에 전달해야 합니다.
1.6	엔드포인트 보호 시스템(EPS) 로그: 로그를 CloudWatch Logs 로그 그룹에 전달하도록 EPS 솔루션 로깅을 활성화하고 구성해야 합니다.
1.7	애플리케이션 로그: 고객은 애플리케이션에서 로깅을 활성화하고 CloudWatch Logs 로그 그룹 또는 S3 버킷에 저장할 수 있습니다.
1.8	S3 객체 수준 로깅: 고객은 S3 버킷에서 객체 수준 로깅을 활성화할 수 있습니다.

ID	기술 표준
1.9	서비스 로깅: 고객은 모든 핵심 서비스와 같은 SSPS 서비스에 대한 로그를 활성화하고 전달할 수 있습니다.
1.10	Elastic Load Balancing(Classic/Application Load Balancer/Network Load Balancer) 로그: 액세스 및 오류 로그 항목은 AMS 2.0 관리형 S3 버킷에 저장되어야 합니다.
2.0	액세스 제어
2.1	로그 및 CloudWatch Logs; 로그 그룹을 저장하는 AMS에 필요한 S3 버킷에는 쓰기 또는 삭제 액세스 권한이 없어야 합니다.
2.2	계정의 모든 로그에 대한 읽기 전용 액세스 권한이 있어야 합니다.
2.3	로그를 저장하는 AMS 필수 S3 버킷은 타사 계정 사용자를 버킷 정책의 원칙으로 허용해서는 안 됩니다.
2.4	승인된 보안 담당자의 명시적 승인 없이 CloudWatch Logs 로그 그룹의 로그를 삭제해서는 안 됩니다.
3.0	로그 보존
3.1	AMS 필수 CloudWatch Logs 로그 그룹의 로그 보존 기간은 최소 90일이어야 합니다.
3.2	로그를 저장하는 AMS 필수 S3 버킷의 최소 보존 기간은 로그에서 18개월이어야 합니다.
3.3	AWS Backup 스냅샷은 지원되는 리소스에서 최소 31일 동안 보존할 수 있어야 합니다.

ID	기술 표준
4.0	암호화(Encryption)
4.1	로그를 저장하는 AMS Teams에 필요한 모든 S3 버킷에서 암호화를 활성화해야 합니다.
4.2	고객 계정에서 다른 계정으로 로그를 전달하는 것은 암호화되어야 합니다.
5.0	무결성
5.1	로그 파일 무결성 메커니즘을 활성화해야 합니다. "로그 파일 검증"은 AMS 팀에 필요한 AWS CloudTrail 추적에서 구성해야 합니다.
6.0	로그 전달
6.1	모든 로그는 한 AMS 계정에서 동일한 고객의 다른 AMS 계정으로 전달할 수 있습니다.
6.2	비 AMS 계정을 동일한 AMS 고객이 소유한 경우에만 모든 로그를 AMS에서 비 AMS 계정으로 전달할 수 있습니다.
6.3	고객 계정의 로그는 타사 계정(고객이 소유하지 않은 계정)으로 전달해서는 안 됩니다.

AMS-STD-008 - AMS-MAD

다음은 008 - AMS-MAD에 대한 표준 컨트롤입니다.

ID	기술 표준
1.0	액세스 관리
1.1	대화형 로그인 및 자동화 작업이 있는 AMS 권한이 있는 사용자만 고객 계정에서 관리형 AD를

ID	기술 표준
	관리하기 위해 관리 호스트에 로그인할 수 있어야 합니다.
1.2	AD 관리자는 위임된 관리자 권한(AMS 위임된 관리자 그룹)만 있어야 합니다.
1.3	고객 AD 환경(관리 호스트 또는 인스턴스)에 로그인하는 엔지니어는 시간 제한 액세스 권한이 있어야 합니다.
1.4	고객은 EC2 인스턴스에서 원격 서버 관리자 도구를 사용하여 AD 객체에 대한 읽기 전용 액세스 권한을 가집니다.
1.5	Active Directory 사용자 또는 그룹에 대한 관리 권한은 허용되지 않아야 합니다.
1.6	AWS 동일한 고객이 AWS 계정 소유한 와의 디렉터리 공유는 위험 알림과 함께 허용됩니다.
2.0	서비스 계정
2.1	그룹 관리형 서비스 계정(gMSA)은 표준 서비스 계정 대신 애플리케이션에서 지원하는 모든 곳에서 사용해야 합니다.
2.2	다른 모든 서비스 계정은 위험 수락 프로세스 후에 생성해야 합니다.
2.3	AD 보안 그룹은 고객이 명시적으로 요청하지 않는 한 재사용해서는 안 됩니다. 새 AD 그룹을 생성해야 합니다. 서비스 계정에 대한 액세스를 요청하는 컴퓨터 객체를 새 보안 그룹에 추가해야 합니다.
2.4	모든 gMSA 서비스 계정(들)은 "관리형 서비스 계정" 조직 단위(OU) 아래에 추가해야 합니다.

ID	기술 표준
2.5	gMSA가 아닌 서비스 계정(들)은 "Users\Service Accounts" OU 아래에 추가해야 합니다.
3.0	그룹 정책 객체(GPO)
3.1	"Windows Settings > Security Settings" GPO 아래의 설정은 현재 상태에서 어떤 방식으로든 계정의 보안 태세를 저하시키는 경우 수정해서는 안 됩니다.
3.2	GPO 생성을 요청하는 애플리케이션 계정에서 제출된 RFCs인 MALZ에서는 GPO를 앱 계정에 해당하는 OU에 연결해야 합니다. 모든 계정에 영향을 미치는 모든 GPOs는 공유 서비스 계정에서 가져와야 합니다.
3.3	활성 디렉터리 도메인의 모든 서버에 대해 기본 RDP 유휴 세션 제한 시간을 15분으로 설정해야 합니다.
4.0	Active Directory 신뢰
4.1	조건부 전달자의 IPs가 DX, VPC-peer 또는 VPN을 통해 VPC로 라우팅되는 경우 단방향 아웃바운드 신뢰(AMS 호스팅 디렉터리에서 고객 디렉터리로)가 허용됩니다.
5.0	기타
5.1	로그 파일 무결성 메커니즘을 활성화해야 합니다. "로그 파일 검증"은 AMS 팀에 필요한 AWS CloudTrail 추적에서 구성해야 합니다.
6.0	로그 전달

ID	기술 표준
6.1	고객 사용자, 그룹, 컴퓨터 객체, OU 또는 기타 엔터티는 AMS 명명 규칙에 따라 AMS 명명 규칙을 사용해서는 안 됩니다.
6.2	모든 OUs AMS에서 관리해야 합니다.

AMS-STD-009 - 기타

다음은 009 - 기타에 대한 표준 컨트롤입니다.

- 리소스, 객체, 데이터베이스 또는 파일 시스템에서 암호화가 활성화된 경우 암호화를 비활성화해서는 안 됩니다.

환경에서 보안 위험이 높거나 매우 높은 변경 사항

다음과 같은 변경 사항으로 인해 환경에서 보안 위험이 높거나 매우 높습니다.

AWS Identity and Access Management

- High_Risk-IAM-001: 루트 계정에 대한 액세스 키 생성
- High_Risk-IAM-002: 추가 액세스를 허용하는 SCP 정책 수정
- High_Risk-IAM-003: AMS 인프라를 손상시킬 수 있는 SCP 정책 수정
- High_Risk-IAM-004: 고객 계정에서 인프라 변경 권한(쓰기, 권한 관리 또는 태그 지정)이 있는 역할/사용자 생성
- High_Risk-IAM-005: IAM 역할은 AMS 계정과 타사 계정(고객이 소유하지 않음) 간의 정책을 신뢰합니다.
- High_Risk-IAM-006: 타사 계정을 통해 AMS 계정에서 모든 KMS 키에 액세스하기 위한 교차 계정 정책
- High_Risk-IAM-007: 데이터를 저장할 수 있는 AMS 고객 S3 버킷 또는 리소스(예: Amazon RDS, Amazon DynamoDB 또는 Amazon Redshift)에 액세스하기 위한 타사 계정의 교차 계정 정책
- High_Risk-IAM-008: 고객 계정의 인프라 변경 권한을 사용하여 IAM 권한 할당
- High_Risk-IAM-009: 계정의 모든 S3 버킷에 대한 나열 및 읽기 허용
- High_Risk-IAM-010: 읽기/쓰기 권한이 있는 자동화된 IAM 프로비저닝

네트워크 보안

- High_Risk-NET-001: 인터넷에서 OS 관리 포트 SSH/22 또는 SSH/2222(SFTP/2222 아님), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 또는 1604, LDAP/389 또는 636 및 NETBIOS/137-139를 엽니다.
- High_Risk-NET-002: 데이터베이스 관리 포트 MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433 또는 인터넷의 모든 관리 고객 포트 열기
- High_Risk-NET-003: 모든 컴퓨팅 리소스에서 직접 애플리케이션 포트 HTTP/80, HTTPS/8443 및 HTTPS/443을 엽니다. 예: 인터넷에서 EC2 인스턴스, ECS/EKS/Fargate 컨테이너 등
- High_Risk-NET-004: AMS 인프라에 대한 액세스를 제어하는 보안 그룹에 대한 모든 변경 사항
- High_Risk-NET-006: 타사 계정과의 VPC 피어링(고객이 소유하지 않음)
- High_Risk-NET-007: 고객 방화벽을 모든 AMS 트래픽의 송신 지점으로 추가
- High_Risk-NET-008: 타사 계정과의 Transit Gateway 연결이 허용되지 않음
- High_Risk-S3-001: S3 버킷에서 퍼블릭 액세스 프로비저닝 또는 활성화

로깅

- High_Risk-LOG-001: CloudTrail을 비활성화합니다. (Ops Site Manager 승인 필요)
- High_Risk-LOG-002: VPC 흐름 로그를 비활성화합니다. (Ops Site Manager 승인 필요)
- High_Risk-LOG-003: AMS 관리형 계정에서 타사 계정(고객이 소유하지 않음)으로 모든 메서드(S3 이벤트 알림, SIEM 에이전트 풀, SIEM 에이전트 푸시 등)를 통한 로그 전달
- High_Risk-LOG-004: CloudTrail에 비 AMS 추적 사용

호스트 보안

- High_Risk-HOST-001: 어떤 이유로든 계정에서 엔드포인트 보안을 비활성화합니다.(Ops Site Manager 승인 필요)
- High_Risk-HOST-002: 리소스 또는 계정 수준에서 패치 적용을 비활성화합니다.
- High_Risk-HOST-003: 계정에 비관리형 EC2 인스턴스 배포.
- High_Risk-HOST-004: 고객이 제공하는 사용자 지정 스크립트 실행.
- High_Risk-HOST-005: 인스턴스에서 로컬 관리자 계정 생성.
- High_Risk-HOST-006: Trend Micro EPS 파일 유형/확장 스캔 제외 또는 엔드포인트에서 맬웨어 방지 비활성화.

 Note

침투 테스트, 취약성 스캔 또는 선제적 조치가 필요한 이벤트에 영향을 미치는 서비스/알려진 성능 문제와 관련된 EPS 맬웨어 방지 제외 또는 GuardDuty 억제 규칙에는 위험 수락이 필요하지 않습니다. 이러한 상황에서는 위험 알림으로 충분합니다.

- High_Risk-HOST-007: EC2용 KeyPair 생성
- High_Risk-HOST-008: EC2에서 엔드포인트 보안 비활성화
- High_Risk-HOST-009: 수명 종료(EOL) OS를 사용하는 계정

기타사항

- High_Risk-ENC-001: 활성화된 경우 모든 리소스에서 암호화 비활성화

관리형 Active Directory

- High_Risk-AD-001: 활성 디렉터 사용자 또는 그룹에 관리자 권한 제공
- High_Risk-AD-002: 계정의 보안 태세를 줄일 수 있는 GPO 정책

AMS Advanced의 연속성 관리

AWS Managed Services(AMS)는 연속성 관리의 일환으로 네이티브 서비스 AWS Backup인에 대한 자동화된 액세스를 제공합니다 AWS. 이를 통해 Amazon EBS, Amazon EC2, Amazon RDS, Amazon EFS 등을 지원하는 서비스에 쉽게 액세스할 수 있습니다.

자세한 내용은 [AWS Backup: 작동 방식을 참조하세요](#).

주제

- [연속성 관리란 무엇입니까?](#)
- [연속성 관리 작동 방식](#)
- [재해 복구 응답](#)
- [재해 복구 계획](#)

연속성 관리란 무엇입니까?

연속성 관리는 AMS가 계정에 대한 백업 및 스냅샷을 제공하는 데 사용하는 프로세스입니다.

AMS는 백업 작업 및 계획을 생성하고 관리하는 데 사용하는 변경 유형을 AWS Backup 통해에 대한 액세스를 제공합니다.

연속성 관리 작동 방식

AMS는 연속성 관리를 [AWS Backup](#) 위해를 사용합니다.

AMS AWS Backup 에서 로 작업을 시작하는 경우:

1. 온디맨드 백업 실행
2. 백업 계획 생성(선택 사항, AMS에서 기본 백업 계획 제공)
3. 기본 AMS를 백업 볼트로 사용(선택 사항)
4. 백업 계획 및 복구 시점 관리(실행, 구체화, 삭제 등)

AMS 백업 계획

백업 계획은 RDS 데이터베이스, EBS 볼륨, DynamoDB 테이블 및 EFS 파일 시스템과 같은 지원되는 AWS 리소스를 백업할 시기와 방법을 정의하는 정책 표현식입니다. 예약 및 보존 정책은 AMS

Advanced에서 변경 유형(CT)을 사용하거나 AMS Accelerate에서를 사용하여 생성할 수 AWS Backup 있는 사용자 지정 백업 계획을 통해 관리됩니다. 태그를 사용하여 백업 계획에 리소스를 할당하고 정의된 백업 계획에 따라 할당된 리소스에 대한 백업을 AWS Backup 자동으로 백업하고 유지합니다. 백업 요구 사항이 다른 워크로드가 있는 경우 여러 백업 계획을 만들 수 있습니다.

백업 계획에는 일정과 보존 기간을 정의하는 백업 규칙이 최대 6개까지 포함될 수 있습니다. 백업 일정에 따라가 백업 작업을 AWS Backup 시작하는 시기와 백업 생성 빈도가 결정됩니다. 시간별, 일별, 주별 또는 월별 빈도를 선택할 수 있습니다. 삭제 일수 설정은 스냅샷이 자동으로 삭제되기 전에 저장되는 일수를 결정합니다.

Note

AMS Advanced: 레거시 AMS 백업 시스템에서 마이그레이션한 경우 AMS는 이전 버전과의 호환성을 위한 기본 백업 계획을 생성합니다. 이 시나리오의 키:값 페어는 Backup:True입니다. 이전 버전과의 호환성을 지원하기 위해 여기서 값은 대/소문자를 구분하지 않으므로 Backup:True 또는 Backup:TRUE는 모두 유효한 태그입니다. 다른 모든 키:값 페어는 대/소문자를 구분합니다.

AWS Backup 는 EBS 볼륨 수준 또는 Amazon EC2 인스턴스 수준에서 작동할 수 있지만 백업이 충돌할 수 있는 경합 조건이 발생할 수 있으므로 두 가지를 동시에 수행할 수는 없습니다.

기본 백업 계획, 다중 계정 랜딩 존

새 계정 생성 RFC 중에 AMS는 워크로드를 보호하기 위해 계정 수준에서 중요한 기본 백업 계획이 있는지 확인합니다. 필수 필드의 값은 다음 섹션과 같이 기본적으로 설정됩니다.

기본 AMS 백업 계획

default-backup-plan

TAG 키: Backup

TAG 값: True

```
RuleForDailyBackups schedule expression: cron(30 23 ? * *) (a daily backup for 23:30 UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(30 23 ? * 7 *) (a weekly backup for 23:30 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
```

```
RuleForMonthlyBackups schedule expression: cron(30 23 * ? *) (a monthly backup for
23:30 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(30 23 1 1 ? *) (a yearly backup for
23:30 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

기본 AMS 백업 계획	Start Time	Retention
hourly backup	N/A	N/A
daily backup	daily 11:30PM UTC	7 days
weekly backup	weekly 11:30PM UTC, only on Saturday	4 weeks
monthly backup	monthly 11:30 PM UTC, on day 1 of the month	26 weeks
yearly backup	11:30 PM UTC, on day 1 of the month	2 years

향상된 기본 AMS 백업 계획

이 계획은 랜섬웨어 공격으로부터 보호하기 위한 AWS Backup 모범 사례를 위한 청사진입니다. 일별, 주별, 월별 및 연간 백업 전략을 구현합니다. AWS Backup [지원되는 리소스에 대해 최대 보존 기간\(31 일\)으로 연속 백업](https://docs.aws.amazon.com/aws-backup/latest/devguide/point-in-time-recovery.html#point-in-time-recovery-supported-services)이 활성화됩니다. <https://docs.aws.amazon.com/aws-backup/latest/devguide/point-in-time-recovery.html#point-in-time-recovery-supported-services>

ams-enhanced-default-backup-plan

TAG 키: backup-orchestrator-enhanced

TAG 값: true

```
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForDailyBackups continuous backup: true
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
UTC time only on Saturday)
```

```
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

향상된 AMS 백업 계획	Start Time	Retention
hourly backup	N/A	N/A
daily backup	daily 4:00 UTC	31 days
weekly backup	Saturday, 2:00 UTC	6 weeks
monthly backup	1st of the month, 2:00 UTC	26 weeks
yearly backup	Jan 1st, 2:00 UTC	2 years

데이터에 민감한 AMS 백업 계획

이 계획은 데이터에 민감한 애플리케이션에 대한 랜섬웨어 공격으로부터 보호하기 위한 AWS Backup 모범 사례를 위한 청사진입니다. 시간별, 일별, 주별, 월별 및 연간 백업 전략을 구현합니다. AWS Backup [연속 백업](#)은 [지원되는 리소스](#)에서 최대 보존 기간(31일)으로 활성화됩니다.

ams-data-sensitive-backup-plan

TAG 키: backup-orchestrator-data-sensitive

TAG 값: true

```
RuleForHourlyBackups schedule expression: cron(0 * ? * * *) (an hourly backup at the
hour mark)
RuleForHourlyBackups delete after days: 7 days
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
```

```
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

데이터에 민감한 AMS 백업 계획	Start Time	Retention
hourly backup	at the hour mark	7 days
daily backup	daily 4:00 UTC	31 days
weekly backup	Saturday, 2:00 UTC	6 weeks
monthly backup	1st of the month, 2:00 UTC	26 weeks
yearly backup	Jan 1st, 2:00 UTC	2 years

AMS 백업 볼트

AWS Backup 는 스냅샷을 볼트라는 논리적 스토리지 단위로 구성합니다.

태그를 사용하여 개별 볼트 수준에서 백업 볼트 알림을 제어할 수 있습니다. 태그를 추가하여 `AMSNotificationOptOut`하고 특정 볼트에서 값을 로 설정하여 특정 볼트 `True`에 대한 알림을 옵트아웃할 수 있습니다. 볼트에서 알림을 다시 받으려면 태그를 제거합니다.

AMS 백업 목록을 보려면 [AWS Backup 콘솔](#)을 엽니다. 탐색 창에서 백업 볼트를 선택하고 다음 표에서 AMS 백업 볼트 중 하나를 선택합니다. 백업 섹션에서 백업 볼트의 모든 백업 목록을 봅니다. 편집, 삭제 또는 복원할 백업을 선택합니다.

AMS 백업 계획을 위한 볼트

AMS 볼트 이름	설명
ams-automated-backups	This vault receives all recovery points taken by the AMS Advanced default AWS Backup plan default-backup-plan.

AMS 볼트 이름	설명
ams-automated-enhanced-backups	This vault receives all recovery points taken by AMS Advanced enhanced default AWS Backup plan ams-enhanced-default-backup-plan.
ams-automated-data-sensitive-backups	This vault receives all recovery points taken by AMS Advanced AWS Backup plan ams-data-sensitive-backup-plan.
ams-manual-backups	This is the default location for all backups from Start Backup Job RFC (ct-2hhud2lx01tq7) backup plans, if no vault name is defined.
ams-custom-backups	This is the default location for the snapshots AMS takes prior to patching an instance using Patch Orchestrator or the monthly patch activities. These are automatically removed according to the AMS patch lifecycle default policy of 60 days.

AMS 백업 변경 유형

AMS는 백업 계획을 생성하고 사용할 수 있는 여러 CTs를 제공합니다.

Important

변경 사항이 손실될 수 있으므로 AMS 기본 백업 계획을 편집하지 마십시오. 대신 사용자 지정 구성에 대한 새 계획을 생성합니다.

- [백업 계획: 생성](#)
- [백업 작업: 시작](#)
- [백업 작업: 중지](#)
- [복구 시점: 삭제](#)
- [DynamoDB | 백업에서 생성](#)

- [EBS 볼륨: 백업에서 생성](#)
- [Amazon Elastic File System\(EFS\): 백업에서 생성](#)

AMS 백업 모니터링 및 보고

Important

AMS 백업 모니터링 및 보고는 AMS 지원 리전에서만 사용할 수 있습니다. 미국 동부(버지니아), 미국 서부(캘리포니아 북부), 미국 서부(오레곤), 미국 동부(오하이오), 캐나다(중부), 남아메리카(상파울루), EU(아일랜드), EU(프랑크푸르트), EU(런던), EU(파리), 아시아 태평양(뭄바이), 아시아 태평양(서울), 아시아 태평양(싱가포르), 아시아 태평양(시드니), 아시아 태평양(도쿄)입니다.

AMS는 리소스 적용 범위 및 백업 작업 상태에 대한 월별 보고서뿐만 아니라 일일 셀프 서비스 보고서를 생성합니다. 월별 보고서는 월별 비즈니스 검토(MBRs. 일일 백업 보고서에 대한 자세한 내용은 [일일 백업 보고서 단원](#)을 참조하십시오.

AMS 전문가를 사용하여 구성된 모든 백업 작업을 모니터링합니다 AWS Backup. 백업 실패 시 AMS는 실패를 조사하고 가능한 경우 근본 원인 및 해결 옵션을 알려줍니다. 알림 노이즈를 방지하기 위해 계정에서 백업 실패 수가 많은 이벤트가 발생하는 경우 AMS는 각 개별 실패에 대해 알리는 대신 CSDM을 통해 집합적 권장 사항을 제공합니다.

AMS는 AWS 서비스의 독립 실행형 백업 기능을 사용하여 구성된 백업을 모니터링하지 않습니다.

재해 복구 응답

다음 섹션에 설명된 옵션 외에도 AMS를 사용하여 재해 복구(DR)를 시작하기 위해 취해야 할 단계를 파악하는 것이 좋습니다.

재해가 발생하여 복구를 시작해야 하는 경우 다음 일반 지침을 따르세요.

1. 가용성 범주를 사용하여 우선순위가 높은 인시던트를 엽니다. AMS가 회의 브리지를 열고 팀에 참여하도록 초대합니다.
2. 복구해야 하는 리소스 목록을 파악합니다.
3. 복구해야 하는 대상 랜딩 존(LZ)(예: 동일한 계정, 다른 AZ 또는 다른 계정 및 다른 리전)을 파악합니다.

- 대상 랜딩 존의 각 리소스에 대한 복구 요청을 제출합니다. 기존 DR 계획을 따르거나 다음 섹션의 옵션(예: [AMS에서 EBS 스냅샷을 사용하는 EC2에 대한 재해 보호](#) 또는 [AMS에서 Elastic Disaster Recovery를 사용하여 EC2에 대한 재해 보호](#))을 참조하세요.
- 애플리케이션 기능을 복원하고 AMS 지원을 사용하여 인프라 관련 문제를 해결합니다.

AMS는 이 이벤트를 준비하고 조직에서 이러한 질문을 처리할 DR 계획을 생성하는 데 도움이 될 수 있습니다. 자세한 내용은 클라우드 서비스 제공 관리자(CSDM) 또는 클라우드 아키텍트(CA)에게 문의하십시오.

재해 복구 계획

재해 복구(DR)는 엔터프라이즈 비즈니스 연속성 및 규정 준수를 위한 중요한 서비스입니다. AMS는 고객과 협력하여 AMS에서 DR 전략을 계획, 구현 및 유지 관리하는 데 도움을 줍니다.

다중 계정 및 단일 계정인 AMS 랜딩 존(LZ)은 대부분의 재해 보호 시나리오를 충족하는 AMS 인프라 구성 요소에 대해 네이티브 다중 AZ 고가용성을 제공합니다. 그러나 비즈니스의 지리적 범위에 따라 리전별 보호가 필요할 수 있습니다. 리전 간 가용성 및 DR의 경우 다른 리전에 다른 AMS 계정이 필요합니다(다중 계정 랜딩 존과 단일 계정 랜딩 존 모두에 해당).

AMS는 이 블로그에 설명된 AWS DR 지침에 따라 [재해 발생 시 미션 크리티컬 시스템을 신속하게 복구](#)하고 다음 네 가지 옵션을 지원합니다.

- 다중 사이트(또는 가용성이 높음)
- 워 스탠바이
- 파일럿 라이트
- 백업 및 복원

이러한 옵션 및 AMS 지원은 다음 섹션에 설명되어 있습니다.

다중 사이트 또는 고가용성(HA)

HA 솔루션은 일반적으로 클러스터링 또는 동기식 복제와 같은 애플리케이션의 내장 기능을 통해 제공됩니다. 사용자는 Prod 노드와 HA/DR 노드로 모두 이동합니다. DNS는 노드를 직접 또는 탄력적 로드 밸런서(ELB)를 통해 가리킵니다.

AMS 클라우드 아키텍트(CA)는 Well-Architected-Review 및 DR 계획의 일환으로 사용자와 협력합니다.

HA DR은 다음 그림과 같이 애플리케이션 및 AWS 네이티브 서비스와 기능을 활용합니다.

DR 사이트는 동일하거나 다를 수 있습니다 AWS 리전.

Note

리전(교차 리전)마다 Active Directory 환경이 다릅니다.

DR(장애 조치) 단계: 자동 장애 조치, 수동 단계는 필요하지 않습니다. 기본 LZ에 장애가 발생하는 경우 사용자는 자동으로 DR/HA 노드로 다시 라우팅됩니다. 이는 DNS 및 애플리케이션 구성 모두에 의해 달성됩니다.

HA DR 지표:

- Recovery Point Objective(RPO): <5분
- Recovery Time Objective and (RTO): <5분
- 유지 관리: 높음(애플리케이션 구성, 패치 적용, SG 또는 ALB, 인증서 등과 같은 두 환경 모두에서 동기식 변경이 필요함).
- 비용: 높음

웜 대기

“웜 스탠바이”라는 용어는 확장 버전의 환경이 클라우드에서 실행되는 재해 복구(DR) 시나리오를 설명하는 데 사용됩니다.

데이터 복제는 애플리케이션 계층에서 일반적으로 온라인 인스턴스로 비동기적으로 처리되는 반면, 나머지 인스턴스(예: 애플리케이션 및 웹 계층)는 비용을 절약하기 위해 꺼질 수 있습니다. 사용자는 프로덕션 사이트로만 이동합니다. 탄력적 로드 밸런서(ELB)와 같은 다른 AWS 리소스도 DR 사이트에서 사전 프로비저닝될 수 있습니다.

AMS Cloud Architect(CA)는 Well-Architected-Review 및 DR 계획의 일환으로 사용자와 협력합니다.

웜 스탠바이 DR은 다음 그림과 같이 애플리케이션 및 AWS 네이티브 서비스와 기능을 활용합니다.

DR 사이트는 동일하거나 다를 수 있습니다 AWS 리전.

Note

리전(교차 리전)마다 Active Directory 환경이 다릅니다.

DR(장애 조치) 단계:

1. 데이터 복제를 중지하고 DR 사이트의 데이터 인스턴스를 마스터로 설정
2. 필요에 따라 애플리케이션 구성 업데이트(새 IP, 서버 이름 등)
3. DNS를 DR 사이트(ELB)로 리디렉션
4. 필요한 경우 AD 종속성(서비스 계정, SPNs, GPOs 등)

HA DR 지표:

- Recovery Point Objective(RPO): <1시간
- Recovery Time Objective and (RTO): <1시간(인스턴스 수 및 오케스트레이션에 따라 다름)
- 유지 관리: 높음(애플리케이션 구성, 패치 적용, 보안 그룹(SG) 또는 애플리케이션 로드 밸런서(ALB), 인증서 등과 같은 두 환경 모두에서 동기식 변경이 필요함).
- 비용: 중간

파일럿 라이트

이 재해 복구(DR) 접근 방식에서는 제한된 코어 서비스 세트에 대해 Prod 환경의 일부를 복제합니다. 인프라의 작은 부분은 항상 실행되며 변경 가능한 데이터(예: 데이터베이스 또는 문서)를 동시에 동기화하는 반면 인프라의 다른 부분은 꺼져 있고 테스트 중에만 사용됩니다. 백업 및 복구 접근 방식과 달리 가장 중요한 코어 요소가 이미 구성되어 있고 DR 랜딩 존(시도등)에서 실행되고 있는지 확인해야 합니다.

AMS 클라우드 아키텍트는 Well-Architected-Review 및 DR 계획의 일환으로 고객과 협력합니다.

Pilot Light DR은 다음 그림과 같이 애플리케이션 및 AWS네이티브 서비스와 기능을 활용합니다.

DR 사이트는 동일하거나 다를 수 있습니다 AWS 리전.

Note

리전(교차 리전)마다 Active Directory 환경이 다릅니다.

DR(장애 조치) 단계:

1. 데이터 복제를 중지하고 DR 사이트의 데이터 인스턴스를 마스터로 설정
2. 꺼진 인스턴스 및 인프라 시작
3. 필요에 따라 애플리케이션 구성 업데이트(새 IP, 서버 이름 등)
4. 필요에 따라 인스턴스를 ELB에 추가
5. DNS를 DR 사이트(ELB)로 리디렉션
6. 필요한 경우 AD 종속성(서비스 계정, SPNs, GPOs 등)

파일럿 라이트 DR 지표:

- Recovery Point Objective(RPO): <1시간
- Recovery Time Objective and (RTO): ~1시간(인스턴스 수 및 오케스트레이션에 따라 다름)
- 유지 관리: 중간
- 비용: 중간

백업 및 복원

이 간단하고 저렴한 재해 복구(DR) 접근 방식은 재해 복구 중에 사용할 수 있도록 어디서나 DR 랜딩 존으로 데이터와 애플리케이션을 백업합니다.

AMS 클라우드 아키텍트는 백업 및 DR 계획의 일부로 사용자와 협력합니다.

Backup and Restore DR은 다음 그림과 같이 AMS 자동 도구 및 프로세스를 활용합니다.

두 가지 백업 및 복제 방법을 사용할 수 있습니다.

- "EBS"라고 하는 EBS 스냅샷(복구 시점 목표(RPO) > 1시간)
- AWS Elastic Disaster Recovery (복구 시점 목표(RPO) ~ 0.25시간), "DRS"라고 함

DR 사이트는 동일하거나 다른에 있을 수 있습니다 AWS 리전.

 Note

다른 리전(교차 리전)에는 다른 Active Directory 환경이 있습니다.

DR(장애 조치) 단계:

1. 스냅샷에서 인스턴스 복원(자리 표시자 인스턴스를 먼저 사용하는 2단계 프로세스)
2. 애플리케이션 구성 업데이트(새 IP, 서버 이름 등)
3. 필요에 따라 다른 인프라 설정(SG, ELB 등)
4. DNS를 DR 사이트(ELB)로 리디렉션
5. 필요한 경우 AD 종속성 업데이트 또는 복원(서비스 계정, 서비스 보안 주체 이름(SPNs), 그룹 정책 객체(GPOs) 등)

DR 지표 백업 및 복원:

- Recovery Point Objective(RPO): >1시간 또는 ~0.25시간(선택한 솔루션에 따라 다름 - EBS 또는 DRE)
- Recovery Time Objective and (RTO): ~1시간(인스턴스 수 및 오케스트레이션에 따라 다름)
- 유지 관리: 높음(애플리케이션 구성, 패치 적용, 보안 그룹 또는 애플리케이션 로드 밸런서, 인증서 등과 같은 두 환경 모두에서 동기식 변경이 필요합니다).
- 비용: 중간

AMS에서 EBS 스냅샷을 사용하는 EC2에 대한 재해 보호

사전 조건:

- AMS Prod 랜딩 존(소스)
- AMS DR 랜딩 존(DR 대상)
- EC2 인스턴스에 대해 EBS 스냅샷이 활성화됨(AWS Backup)

스냅샷 복제 솔루션:

- 교차 AZ: 해당 사항 없음 - EBS 스냅샷은 설계상 리전 내에서 가용성이 높습니다.

- 교차 리전: AWS Backup

다음 다이어그램은 AMS의 EBS 스냅샷에서 EC2 복원 프로세스를 나타냅니다.

AMS의 EC2 DR 단계:

1. RFC를 생성하여 대상 계정과 EBS 스냅샷을 공유합니다(교차 리전 DR에 필요).

: 관리, 고급 스택 구성 요소, EBS 스냅샷, 공유

2. 대상 서브넷(DR 사이트 서브넷)에 자리 표시자 EC2 AMS 스택을 생성합니다. 고객이 동일한 스택에서 보안 그룹 및 기타(예: ELB에 인스턴스 추가)를 할당하는 단계를 결합할 수 있으므로 CFN 수집을 사용하여 스택을 생성하는 것이 좋습니다.

변경 유형: 배포, 수집, CloudFormation 템플릿의 스택, 생성

3. RFC를 열어 EC2 스택 볼륨 복원을 수행합니다.

변경 유형: 관리, 고급 스택 구성 요소, EC2 인스턴스 스택, 볼륨 복원.

CT는 1단계에서 공유된 스냅샷에서 볼륨을 복원하고 2단계에서 생성된 자리 표시자 인스턴스에 연결합니다.

볼륨 복원 CT 기능:

- 자리 표시자 인스턴스 종료
- 스냅샷에서 볼륨 복원
- 볼륨 스왑
- 인스턴스 시작
- 이전 도메인에서 나가기
- 호스트 이름 변경
- 재부팅합니다. AMS 부트스트랩 스크립트는 시작 시 인스턴스를 대상(DR) 도메인에 조인합니다.

볼륨 복원 CT 입력:

- InstanceId(자리 표시자 인스턴스 ID)
- RootDeviceSnapshotId, 복원된 루트 볼륨의 EBS 스냅샷

- EC2 인스턴스에서 복원된 모든 볼륨을 암호화하기 위한 KMSKeyId, KMS 키 식별자 또는 ARN
- DeviceNames, 최대 25개(선택 사항)
- SnapshotIds, 최대 25개(선택 사항). 복원할 볼륨의 스냅샷 목록

AMS에서 Elastic Disaster Recovery를 사용하여 EC2에 대한 재해 보호

사전 조건:

- AMS Prod 랜딩 존(소스)
- AMS DR 랜딩 존(DR 대상)
- 먼저 사용 AWS 리전 하려는 모든에 대해 Elastic Disaster Recovery 서비스를 초기화해야 합니다.

Elastic Disaster Recovery 콘솔 액세스를 위해 DR 랜딩 존(LZ)에 IAM 역할을 생성합니다.

- 중요: SSM 문서는 DRS 내에서 시작 후 작업으로 생성됩니다. 이 작업은 PostLaunch 설정의 모든 서버에서 활성화해야 합니다.
- 대상(자리 표시자) 인스턴스에는 태그 키 "AWSDRS", 값 "AllowLaunchingIntoThisInstance"가 있어야 합니다. 자리 표시자 인스턴스는 중지된 상태여야 합니다. 그렇지 않으면 AMS는 시작 설정에서 자리 표시자 인스턴스를 선택할 수 없고 Elastic Disaster Recovery는 자리 표시자 인스턴스 위에 복원할 수 없습니다.

AMS의 EC2에 대한 Elastic Disaster Recovery 설정 및 복원 프로세스의 다이어그램은 [AWS Elastic Disaster Recovery \(AWS DRS\) 일반 아키텍처](#)를 참조하세요.

AMS에서 Elastic Disaster Recovery를 사용하는 EC2 DR 단계:

1. 적절한 태그를 사용하여 대상 서브넷(DR 사이트 서브넷)에 자리 표시자 EC2 AMS 스택을 생성합니다. 자세한 내용은 이전 섹션을 참조하세요. 동일한 스택에서 보안 그룹을 할당하고 인스턴스, EBS 볼륨 및 기타(예: ELB에 인스턴스 추가)에 태그를 지정하는 단계를 결합할 수 있으므로 CFN 수집을 사용하여 스택을 생성하는 것이 좋습니다.

변경 유형: 배포, 수집, CloudFormation 템플릿의 스택, 생성

2. 자리 표시자 인스턴스를 중지합니다.

변경 유형: 관리, 고급 스택 구성 요소, EC2 인스턴스, 중지

3. 1단계에서 수행하지 않은 경우 자리 표시자 인스턴스와 해당 EBS 볼륨에 키: "AWSDRS", 값: "AllowLaunchingIntoThisInstance"로 태그를 지정합니다.

변경 유형: 관리, 고급 스택 구성 요소, 태그, 업데이트.

4. 소스 서버의 인스턴스 ID로 시작, DRS 시작 설정에서 1단계의 자리 표시자 인스턴스를 대상으로 사용합니다. 소스 서버의 Elastic Disaster Recovery 콘솔에서 인스턴스 복구 드릴을 시작합니다.

 Note

자리 표시자 인스턴스 볼륨은 계정에 유지됩니다. 이러한 볼륨을 삭제하려면 재해 복구 작업이 끝날 때 관리 | 고급 스택 구성 요소 | EBS 볼륨 | 변경 유형 삭제(ct-3e3h8u0sp5z80)를 제출합니다.

Elastic Disaster Recovery 복원 워크플로:

- 대상(자리 표시자) 인스턴스가 중지됨 상태여야 합니다.
- 볼륨을 바꾸고 소스(플레이스홀더) 루트 볼륨을 삭제합니다.
- 인스턴스 시작
- 시작 후 작업을 실행하여 다음 항목을 완료합니다.
 - SSM 에이전트를 활성화합니다.
 - 볼륨을 바꾸고 소스(플레이스홀더) 루트 볼륨을 삭제합니다.
 - 인스턴스 시작
 - PostLaunchScript SSM 문서를 실행합니다. 이 문서는 다음을 수행합니다.
 1. 이전 도메인을 떠납니다.
 2. 호스트 이름을 변경합니다.
 3. 재부팅합니다. AMS 부트스트랩 스크립트는 시작 중에 인스턴스를 대상(DR) 도메인에 조인합니다.

AMS의 패치 관리

주제

- [AMS 패치 오케스트레이터: 태그 기반 패치 적용 모델](#)
- [패치 오케스트레이터 사용](#)
- [온디맨드 패치 적용](#)
- [AMS 표준 패치 적용](#)
- [서비스 커밋 패치 적용](#)

AMS에서 패치 관리는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 OS 공급업체 업데이트를 유지하는 데 도움이 되는 서비스입니다. Amazon EC2 인스턴스 패치의 빈도와 프로세스를 자유롭게 사용자 지정할 수 있습니다.

온보딩 중에 패치 관리를 구성하고 RFC 프로세스를 사용하여 패치를 업데이트할 수 있습니다. 변경 관리 시스템과 패치 호환 템플릿(Amazon EC2, Auto Scaling 그룹, HA 1계층 또는 2계층 스택용)을 사용하여 생성된 스택은 패치 관리를 자동으로 구독합니다.

AMS는 패치 구성을 위한 태그 기반 패치인 패치 오케스트레이터 기능을 제공합니다.

패치 용어에 대한 정의는 섹션을 참조하세요 [AMS 키 용어](#).

Important

- 스택이 생성되는 AMS 템플릿이 패치 관리와 호환되는 경우 스택 또는 스택의 구성 인스턴스가 패치 관리를 옵트아웃할 수 없습니다. 현재 패치 적용은 다음 스택 템플릿과 호환됩니다.
 - Amazon EC2 스택 | 생성 및 Amazon EC2 스택 | 생성(추가 볼륨 포함)
 - AWS CloudFormation 수집으로 시작된 Amazon EC2 인스턴스
 - Auto Scaling 그룹 | 생성(그룹의 Amazon EC2 인스턴스가 패치됨)
 - 고가용성 1계층 스택 | 생성 및 고가용성 2계층 스택 | 생성
- 스택에 영향을 미치는 인시던트가 진행 중인 경우 AMS 운영자는 예약된 패치 적용을 다시 예약하거나 취소할 수 있습니다.
- 기본적으로 특정 패치 호환 스택 내의 모든 인스턴스는 제자리에 패치됩니다. 최신/패치된 AMS AMI를 사용하여 Auto Scaling 그룹에 Amazon Machine Image(AMI) 교체 패치를 적용하려면 서비스 요청을 제출합니다. 업데이트된 AMIs 매월 계정과 공유됩니다.

⚠ Important

관리형 노드에 대한 대체 패치 리포지토리를 지정할 수 있습니다. AMS가 요청된 패치 구성을 구현하는 동안 선택한 리포지토리의 보안을 선택하고 검증할 책임은 사용자에게 있습니다. 또한 공급망 위험과 같이 이러한 리포지토리 사용으로 인한 모든 위험을 수락해야 합니다. 다음은 패치 관리 프로세스의 보안을 위한 모범 사례입니다.

- 신뢰할 수 있고 검증된 리포지토리 소스만 사용
- 가능한 경우 표준 OS 공급업체 리포지토리 기본값
- 사용자 지정 리포지토리 구성을 정기적으로 감사

💡 Tip

AMS는 중요한 애플리케이션 또는 서비스가 있는 인스턴스에 대해 백업을 활성화할 것을 권장합니다. 백업 활성화에 대한 자세한 내용은 섹션을 참조하세요 [AMS Advanced의 연속성 관리](#).

AMS 패치 오케스트레이터: 태그 기반 패치 적용 모델

새 AMS Patch Orchestrator 태그 기반 패치 적용 모델에 온보딩된 경우 태그를 사용하여 한 인스턴스에서 모든 인스턴스에 이르는 패치 그룹이라는 정확한 리소스 세트에 패치 구성을 적용할 수 있습니다. AMS 태그에 대한 자세한 내용은 [태그 사용](#)을 참조하세요. 패치 오케스트레이터 태그 설정에 대한 지침은 다음 섹션에 나와 있습니다.

패치는 [SSM 패치 창 | 생성으로 정의한 패치 기간](#) 중에 설치됩니다. 각 패치 기간은 선택한 일정에 따라 실행되고, 기간이 구성되어 있으며, 하나의 패치 그룹에 적용되는 AWS Systems Manager 유지 관리 기간입니다. 명시적 패치 기간의 일부가 아닌 인스턴스는 패치 오케스트레이터에 온보딩할 때 정의한 기본 유지 관리 기간 동안 패치됩니다.

⚠ Important

여러 패치 유지 관리 기간이 동시에 실행되도록 예약된 경우 지정된 시간에 처리 중인 인스턴스가 1001개 미만이어야 합니다. 이는 AWS Systems Manager 제한 사항입니다. AMS는 인스턴스 50개당 최소 1시간을 권장합니다.

기본적으로 모든 운영 체제(OS) 공급업체 제공 패치는 유지 관리 기간 또는 온디맨드 패치 중에 설치됩니다. 이를 기본 패치 기준이라고 합니다. 설치된 패치를 제한하려면 패치 기준 생성 CTs(OSes) 중 하나를 사용하여 사용자 지정 패치 기준을 정의할 수 있습니다. [패치 하위 범주를 참조하세요](#). 예를 들어 사용자 지정 패치 기준을 사용하여 하나 이상의 패치 그룹에 대해 중요하고 중요한 보안 업데이트만 설치할 수 있습니다.

인스턴스에 패치가 설치되면 인스턴스가 재부팅됩니다. 패치 알림은 패치 적용 후후에 전송되며 예정된 시작 전 96시간 이내에 추가 알림이 전송됩니다. 또한 AMS는 선택한 유지 관리 기간 동안 인프라 관리 도구(예: AWS SSM 에이전트)에 업데이트를 적용합니다.

Important

AMS는 누락된 패치가 있는 인스턴스의 월별 패치 규정 준수 보고를 더 이상 사용하지 않으며 월별 보고서를 보내지 않습니다. 이 변경은 24시간마다 새로 고쳐지고 온디맨드로 사용할 수 있으며 가장 최신의 세분화된 데이터를 제공하는 최근에 릴리스된 셀프 서비스 운영 보고서를 고려하여 이루어졌습니다. 보고서에 대한 자세한 내용은 셀프 서비스 보고를 참조하세요. 보고서에 대한 자세한 내용은 섹션을 참조하세요 [셀프 서비스 보고서](#).

알림에 대한 자세한 내용은 섹션을 참조하세요 [패치 알림](#).

패치 오케스트레이터 사용

다음 세부 정보가 포함된 서비스 요청을 제출하여 계정에 대해 AMS Patch Orchestrator를 활성화합니다.

- 범주: 기타
- 제목: 패치 오케스트레이터에 온보딩
- CC 이메일: CC 이메일 주소는 이 온보딩 RFC의 상태가 변경될 때 알림을 받습니다.
- 세부 정보: 다음 정보를 이메일에 붙여넣고 값을 입력합니다. ThirdTagKey는 선택 사항입니다. 권장 사항 및 예제는 다음 표를 참조하세요.

```
Default maintenance window Schedule:
Default Maintenance Window Schedule TimeZone:
Default Maintenance Window Duration:
Default Maintenance Window Cutoff:
Default Patch Backup Retention In Days:
Default Maintenance Window Notification Emails:
First Tag Key:
```

Second Tag Key:

Third Tag Key:

다음 표에서는 제공된 값의 형식과 권장 사항을 설명합니다.

패치 오케스트레이터 태그 기반 패치 구성

파라미터 이름	정보	권장 사항 또는 예제
기본 유지 관리 기간 일정	cron 또는 rate 표현식 형태의 기본 유지 관리 기간의 일정입니다. 예: • <code>cron(0 3 ? * 6L *)</code>: 매 월 마지막 금요일 오전 3시 • <code>rate(7 days)</code>: 7일마다 cron 표현식 생성 및 cron 및 rate 표현식 리소스에 대한 링크에 대한 자세한 내용은 유지 관리 기간의 Cron 및 rate 표현식을 참조하세요.	일관된 평일에 한 달에 한 번 이상 기간을 실행하는 것이 좋습니다.
기본 유지 관리 기간 일정 시간대	기본 유지 관리 기간이 실행되는 시간대는 IANA(Internet Assigned Numbers Authority) 형식을 기반으로 합니다.	예: • <code>America/Los_Angeles</code> • <code>etc/UTC</code>
기본 유지 관리 기간	기본 유지 관리 기간의 지속 시간입니다.	인스턴스 50개당 최소 1시간, 컷오프의 경우 2시간.
기본 유지 관리 기간 컷오프	새 패치 적용 명령이 시작되지 않는 기본 유지 관리 기간이 끝나기 전의 시간입니다. 이 간격은 기간이 끝나기 전에 패치 적용이 완료될 때까지 충분한 시간을 허용하기 위해 존재합니다.	최소 2시간.

파라미터 이름	정보	권장 사항 또는 예제
기본 패치 백업 보존 일수(선택 사항)	인스턴스를 패치하기 전에 생성된 EBS 복원 지점을 유지하기 위한 일 단위의 기본 시간입니다.	기본값인 60을 유지하는 것이 좋습니다.
기본 유지 관리 기간 알림 이메일	기본 유지 관리 기간 패치 상태에 대한 알림을 수신할 이메일 주소 또는 배포 목록 1~5개.	개별 이메일 대신 그룹 배포 목록을 사용하는 것이 좋습니다.
첫 번째 태그 키	패치 그룹 태그 값을 생성하는데 사용할 첫 번째 태그 키입니다.	AppId. 패치 그룹 태그로 자체 패치 그룹을 이미 정의한 경우 null을 지정합니다.
두 번째 태그 키	패치 그룹 태그 값을 생성하는데 사용할 두 번째 태그 키입니다.	예: 환경. 패치 그룹 태그로 자체 패치 그룹을 이미 정의한 경우 null을 지정합니다.
세 번째 태그 키(선택 사항)	패치 그룹 태그 값을 생성하는데 사용할 선택적 세 번째 태그 키입니다.	예: 그룹.

새 패치 오케스트레이터 패치 서비스 모델에 온보딩된 후 계정에서 적절하게 태그가 지정된 모든 인스턴스는 패치 그룹 태그가 있는 패치 그룹에 속합니다. 패치 오케스트레이터는 기존 패치 그룹 태그 또는 패치 오케스트레이터 온보딩 중에 지정한 두 개 또는 세 개의 연결된 태그 값으로 구성된 AMS 생성 태그를 사용합니다. 예: `{Tag Value 1}{Tag Value 2}{Tag Value 3}`. AMS는 이러한 AMS 적용 패치 그룹 태그를 12시간마다 업데이트합니다. 필요한 경우 태그 [업데이트\(검토 필요\) 또는 태그 업데이트\(검토 필요\) 변경 유형을 사용하여 패치 그룹 태그 값을 업데이트할](#) 수 있습니다.

예를 들어 Amazon EC2 인스턴스에 다음과 같은 태그 키:값 페어가 있는 경우:

- AppId:MyApplication
- Environment:Production
- Group:1

온보딩 중에 다음 태그 키를 지정했습니다.

- First Tag Key = AppId
- Second Tag Key = Environment
- Third Tag Key = Group

AMS는 패치 그룹 태그를 생성하여 인스턴스에 적용합니다 Patch Group:MyApplication-Production-1.

Note

지원되지 않는 운영 체제가 있거나 유지 관리 기간 동안 중지된 인스턴스에 대해서는 패치 실패 알림이 생성되지 않습니다.

패치 오케스트레이터 사전 조건

패치 오케스트레이터 워크플로는 최신 버전의 System Manager Automation Document: AWSManagedServices-PatchInstanceFromMaintenanceWindow로 패치된 Amazon EC2 인스턴스를 대상으로 합니다.

문서 워크플로의 일부로 실행 명령 문서 "AWS-RunPatchBaseline"은 패치 그룹 멤버 중 각 Amazon EC2 인스턴스에 대해 실행됩니다. 자세한 내용은 [SSM 문서 AWS-RunPatchBaseline 정보를 참조하세요](#).

요구 사항:

- AMS 제공 Amazon Machine Image(AMI) 또는 "마이그레이션 파트너의 스택 마이그레이션 인스턴스" CT(ct-257p9zjk14ija)를 통해 AMI에 배포된 Amazon EC2 인스턴스입니다.
- 송신 인터넷 연결이 활성화되었습니다. 방화벽/프록시 솔루션의 경우 Windows 업데이트 엔드포인트 및/또는 Linux 리포지토리 미러 엔드포인트, AWS 시스템 관리자 프록시 설정 및 메타데이터 프록시 구성을 허용해야 합니다. 자세한 내용은 [프록시를 사용하도록 SSM 에이전트 구성](#) 및 [HTTP 프록시 사용을 참조하세요](#).
- IAM 역할의 SSM 서비스에 대한 최소 허용 액세스와 일치하는 customer-mc-ec2-instance-profile IAM 역할입니다.
- 사용 가능한 루트 파티션 공간은 10GB가 좋습니다. Linux OS의 경우 /var 파티션에서 최소 2GB를 사용할 수 있습니다.
- 업데이트 다운로드를 위한 유효한 인증 기관입니다.

- Windows Server Update Services(WSUS) - DisableWindowsUpdateAccess, NoWindowsUpdate를 포함하되 이에 국한되지 않는 레지스트리입니다. 자동 업데이트는 Windows 업데이트 프로세스의 작동을 손상시키지 않아야 합니다.

검증:

- yum 패키지 관리자를 사용하는 Linux OS 인스턴스의 경우를 실행하여 업데이트 가용성을 검증할 수 있습니다. `#yum check-update`
- Linux OS RedHat 5.7 이상, 6.1 이상, 7.0 이상, Amazon EC2 인스턴스가 "마이그레이션 파트너 마이그레이션 인스턴스의 스택" CT(ct-257p9zjk14ija)를 통해 AMS 계정으로 마이그레이션된 경우 업데이트 성능을 위해 구독 관리자 상태를 검증해야 합니다.
- Windows OS에서 Windows Server Update Services(WSUS)를 활성화합니다. 로컬 정책은 업데이트를 스캔하거나 설치하는 WSUS 기능을 차단해서는 안 됩니다. 관리자로 로그인되면 Windows Update Service 콘솔에서 사용 가능한 업데이트를 스캔하여 검증할 수 있습니다. 2012R2, 2016 및 2019를 포함한 Windows Server OS 릴리스에는 다운로드 및 설치에 대한 기본 Windows 업데이트 설정이 있습니다. 스캔 전에 원하는 설정을 구성할 수 있습니다. 이후 OS 릴리스에서 작업은 설치를 트리거하고 원하는 동작을 미리 구성할 수 있습니다.
- '패치 준비 상태 평가를 위해 Amazon EC2 인스턴스에 대해 실행하기 위한 AWSManagedServices-CheckPatchingPrerequisites Automation 문서' 서비스 요청을 제출하여 AMS 운영 팀의 검증을 요청합니다.

Note

지원되지 않는 운영 체제가 있거나 유지 관리 기간 동안 중지된 인스턴스에 대해서는 패치 실패 알림이 생성되지 않습니다.

패치 창

특정 패치 그룹의 인스턴스는 하나 이상의 패치 기간 동안 패치됩니다. 패치 기간은 cron 또는 rate 표현식으로 정의된 일정에 따라 실행되며 선택한 시간 간격 내에 패치 관련 종단을 유지하기 위한 구성 가능한 기간이 있습니다. AMS는 조직의 특정 패치 루틴과 일치시키고 기본 유지 관리 기간을 대체로 사용하도록 모든 인스턴스를 집합적으로 포함하는 여러 패치 기간을 생성하는 것이 좋습니다. 패치 기간은 RFC 변경 유형 배포 | 패치 적용 | SSM 패치 창 | 생성(ct-0el2j07llrxs7)으로 생성됩니다. 패치 기간의 일부가 아닌 모든 인스턴스는 온보딩 중에 생성된 기본 유지 관리 기간 동안 패치됩니다.

일반적으로 패치 기간은 새 인스턴스를 포함하도록 업데이트할 필요가 없습니다. 일반적으로 인스턴스 태그를 수정하여이 작업을 수행합니다. 예를 들어 다음과 같은 이벤트 시퀀스를 고려합니다.

1. 두 인스턴스에는 AppId:MyApplication, Environment:Production, 태그가 지정됩니다Group:1.

그러면 첫 번째 태그 키 = AppId, 두 번째 태그 키 = 환경, 세 번째 태그 키 = 그룹이 생성되고 MyApplication-Production-1 패치 그룹에 대한 패치 창이 생성된다고 가정하여 이러한 인스턴스에 태그가 생성됩니다.

2. 세 개의 인스턴스가 추가로 생성되고 AppId:MyApplication, Environment:Production, 로 태그가 지정됩니다Group:1.

이렇게 하면 패치 그룹:MyApplication-Production-1에 대한 태그가 생성됩니다.

패치 기간은 예약된 다음 실행 시 5개의 인스턴스를 모두 선택하므로 변경할 필요가 없습니다.

이 변경 유형 사용에 대한 자세한 설명과 연습은 [SSM 패치 창 | 생성](#)을 참조하세요.

패치 알림

Important

2025년 2월 1일부터 AMS 고객은 더 이상 관리형 계정의 빈 패치 유지 관리 기간에 대한 알림을 받지 않습니다.

구독한 이메일 주소(최대 5개)는 패치 유지 관리 기간이 시작되기 직전에 다음과 유사한 이메일을 수신합니다.

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME was started at:
2020-02-21T12:02:18.196Z.
Details:
Maintenance Window AccountId: YOUR_ACCOUNT_ID
Maintenance Window Region: YOUR_ACCOUNT_REGION
Maintenance Window Id: THE_MAINTENANCE_WINDOW_ID
Maintenance Window Name: THE_MAINTENANCE_WINDOW_NAME
Maintenance Window Description: MaintenanceWindow for patching patch
Group PATCH_GROUP_NAME
Maintenance Window Patch Group: PATCH_GROUP_NAME
```

Maintenance Window ExecutionId: *THE_EXECUTION_ID*

Targets:

InstanceId	InstanceName	StackId
-----	-----	-----
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>

A follow-up message with a detailed report is sent as soon as the maintenance window is over.

Please raise a service request if you have any inquiries about AMS Patch Orchestrator by following this URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

패치 활동이 끝나면 구독한 이메일 주소는 다음과 유사한 이메일을 수신합니다.

Dear Customer,

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* ended at:
2020-02-21T12:03:20.058Z, with status: SUCCESS.

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
Maintenance Window Region: *YOUR_ACCOUNT_REGION*
Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*
Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*
Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*
Maintenance Window ExecutionId: *THE_EXECUTION_ID*

Targets:

RfcId	InstanceId	InstanceName	StackId
Status			
-----	-----	-----	-----
<i>THE_RFC_ID</i>	<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>
<i>STATUS</i>			

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

Please raise an Incident if an issue is impacting one of your production applications by following this URL:

<https://console.aws.amazon.com/managedservices/incident/new>

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

AMS 패치 시스템은 96시간마다 해당 96시간 내에 예정된 모든 패치 관리형 유지 관리 기간을 식별하고 해당 96시간 기간 내에 속하는 구독한 모든 이메일 주소로 알림 알림을 보냅니다. 기간은 최소 1시간 전 또는 전체 96시간일 수 있습니다. 예:

Dear Customer,

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* will start at:
2020-05-06T16:35:36.523Z.

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
Maintenance Window Region: *YOUR_ACCOUNT_REGION*
Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*
Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*
Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*
Maintenance Window Next Start Time: 2020-05-06T16:35:36.523Z
Maintenance Window Schedule: rate(24 hours)
Maintenance Window Timezone: *THE_TIMEZONE*

At this time, these are the instances in the "*PATCH_GROUP_NAME*" Patch Group:

InstanceId	InstanceName	StackId	InstanceState

<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped
<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>	running/stopped

A notification message is sent as soon as the maintenance window starts.

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

```
https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION
```

If you would like to disable this maintenance window or you have inquires about the AMS Patch Orchestrator click on the following URL:

```
https://console.aws.amazon.com/managedservices/servicerequest/new
```

If you would like to delete this maintenance window, you can run the CT with id "ct-0q0bic0ywqk6c" against the stack id "stack-rctyznutkyj4tkkzq".

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

패치 기준

기본적으로 모든 운영 체제(OS) 공급업체 제공 패치는 AMS 기본 패치 기준을 사용하여 설치됩니다. 설치된 패치를 제한하려면 선택적으로 RFC 변경 유형 배포 | 패치 적용 | SSM 패치 기준 | **OS** 생성(CT ID는 운영 체제에 따라 다름)을 사용하여 패치 기준을 생성할 수 있습니다.

이러한 변경 유형 사용에 대한 자세한 내용은 [패치 하위 카테고리를 참조하세요](#).

패치 오케스트레이터 예약 태그

패치 오케스트레이터는 수정할 수 없는 다음 태그도 생성합니다.

- **AMSPatchGroup** -이 태그는 패치 그룹 태그 값 생성에 사용됩니다. **AMSPatchGroup**을 수정해서는 안 됩니다. 사용자 지정 "패치 그룹" 값을 사용하려면 "패치 그룹" 태그를 수정할 수 있습니다. 패치 오케스트레이터는 온보딩 중에 제공된 태그 키를 기반으로 **AMSPatchGroup** 값을 계속 생성하지만 사용자가 사용자 지정 값으로 설정한 경우 "패치 그룹" 태그 값을 수정하지 않습니다. 사용자 지정 "패치 그룹" 값 사용을 중지하려면 **AMSPatchGroup** 태그 값과 일치하도록 "패치 그룹" 값을 설정할 수 있습니다.
- **AMSDefaultPatchGroup** -이 태그는 인스턴스가 기본 유지 관리 기간의 일부이고 값이 True 또는 False인지 여부를 나타냅니다. 인스턴스의 패치 그룹이 유지 관리 기간에 할당되지 않은 경우이 값은 True로 설정됩니다.

온디맨드 패치 적용

AMS에는 패치 기준과 함께 작동하는 변경 유형이 있으므로 온디맨드 인스턴스에서 패치를 실행할 수 있습니다. 이는 대기 중에서 설정한 기본 기준이거나 패치 기준 변경 유형으로 설정한 Patch Orchestrator Systems Manager 패치 기준일 수 있습니다(CT ID는 운영 체제에 따라 다름).

패치 오케스트레이터를 사용하거나 사용하지 않고 온디맨드 패치 변경 유형을 사용할 수 있습니다.

이 변경 유형 사용에 대한 자세한 내용은 [온디맨드 패치 적용 | 실행을 참조하세요](#).

Note

온디맨드 패치 적용 변경 유형에서는 Auto Scaling 그룹의 일부인 인스턴스를 사용할 수 없습니다.

AMS 표준 패치 적용

AMS는 AMS 표준 패치 모델을 사용하는 기존 고객을 지원하지만 이 모델은 신규 고객에게는 제공되지 않으며 AMS 패치 오케스트레이터를 위해 사용 중지되고 있습니다.

AMS 표준 패치 적용에 대한 일반적인 패치 콘텐츠에는 지원되는 운영 체제 및 지원되는 운영 체제(예: IIS 및 Apache Server)가 사전 설치된 소프트웨어에 대한 공급업체 업데이트가 포함됩니다.

AMS 온보딩 중에 패치 요구 사항, 정책, 빈도 및 기본 패치 기간을 지정합니다. 이러한 구성을 사용하면 인프라 패치 적용을 위해 애플리케이션을 한 번에 모두 오프라인으로 전환하지 않아도 되므로 패치가 적용되는 인프라를 제어할 수 있습니다.

Note

이 주제에 설명된 패치 적용 프로세스는 스택에만 적용됩니다. AMS 인프라는 별도의 프로세스 중에 패치됩니다. AWS Managed Services 유지 관리 기간(또는 유지 관리 기간)은 AWS Managed Services(AMS)에 대한 유지 관리 활동을 수행하고 태평양 표준시로 매월 두 번째 목요일 오후 3시부터 오후 4시까지 반복됩니다. AMS는 48시간 전에 통지하여 유지 관리 기간을 변경할 수 있습니다. 온보딩 시 AMS 패치 기간을 구성하거나 월별 패치 서비스 알림을 승인하거나 거부합니다.

AMS는 관리형 Amazon EC2 인스턴스에서 운영 체제 업데이트 기능을 통해 사용 가능한 업데이트를 정기적으로 스캔합니다. 또한 환경에서 지원되는 AMS 기본 Amazon Machine Image(AMIs)에 대한 정기적인 업데이트를 제공합니다.

검증되면 AMS AMI 릴리스가 모든 AMS 계정과 공유됩니다. [DescribeImages](#) Amazon EC2 API 호출을 사용하거나 Amazon EC2 콘솔을 사용하여 사용 가능한 AWS AMI 릴리스를 볼 수 있습니다. 사용 가능한 AMS AMIs [AMI IDs](#) [AMS 찾기](#).

AMS는 사용자가 요청한 경우에만 임시 패치 적용 일정을 수행합니다. 이전에는 AMS가 알림을 보내지만 현재는 알림이 전송되지 않습니다.

Note

기본적으로 AMS는 Systems Manager를 사용하여 패키지 관리자(Linux) 또는 시스템 업데이트 서비스(Windows)가 기본 리포지토리를 쿼리하여 사용 가능한 새 패키지를 확인하도록 하여 패치를 적용합니다. day-to-day 작업 중에 기본 패키지 관리자를 사용하여 Linux 호스트에 패키지를 설치한 경우 해당 패키지 관리자는 사용 가능한 경우 해당 소프트웨어에 대한 새 패키지도 픽업합니다. 이 경우 패치 작업(이 섹션에 설명됨)을 수행하여 해당 인스턴스에 대해 업데이트할 수 있습니다.

지원되는 운영 체제

지원되는 운영 체제(x86-64)

- Amazon Linux 2023
- Amazon Linux 2(예상 AMS 지원 종료일 2026년 6월 30일)
- Oracle Linux 9.x, 8.x
- Red Hat Enterprise Linux(RHEL) 9.x, 8.x
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server for SAP 15 SP3 이상
- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

지원되는 운영 체제(ARM64)

- Amazon Linux 2023
- Amazon Linux 2(예상 AMS 지원 종료일 2026년 6월 30일)

지원되는 패치

AWS Managed Services는 주로 운영 체제 수준에서 패치 적용을 지원합니다. 설치된 패치는 운영 체제에 따라 다를 수 있습니다.

Important

모든 업데이트는 인스턴스에 구성된 Systems Manager 패치 기준 서비스 원격 리포지토리에서 다운로드되며이 주제의 뒷부분에서 설명합니다. 패치 적용을 수행하려면 인스턴스가 리포지토리에 연결할 수 있어야 합니다.

유지 관리하려는 패키지를 전달하는 리포지토리에 대한 패치 기준 서비스를 옵트아웃하려면 다음 명령을 실행하여 리포지토리를 비활성화합니다.

```
yum-config-manager DASHDASHdisable REPOSITORY_NAME
```

다음 명령을 사용하여 현재 구성된 리포지토리 목록을 검색합니다.

```
yum repolist
```

- Amazon Linux 사전 구성된 리포지토리(일반적으로 4개):

리포지토리 ID	리포지토리 이름
amzn-main/latest	amzn-main-Base
amzn-updates/latest	amzn-updates-Base
epel/x86_64	Enterprise Linux 6용 추가 패키지 - x86_64
pbis	PBIS 패키지 업데이트

- Red Hat Enterprise Linux 사전 구성된 리포지토리(Red Hat Enterprise Linux 7의 경우 5개, Red Hat Enterprise Linux 6의 경우 5개):

리포지토리 ID	리포지토리 이름
rhui-REGION-client-config-server-7/x86_64	Red Hat Update Infrastructure 2.0 클라이언트 구성 Ser
rhui-REGION-rhel-server-releases/7Server/x86_64	Red Hat Enterprise Linux Server 7
rhui-REGION-rhel-server-releases/7Server/x86_64	Red Hat Enterprise Linux Server 7 RH Common(RPMs)
epel/x86_64	Enterprise Linux 7용 추가 패키지 - x86_64
pbis	PBIS 패키지 업데이트

리포지토리 ID	리포지토리 이름
rhui-REGION-client-config-server-6	Red Hat 업데이트 인프라 2.0
rhui-REGION-rhel-server-releases	Red Hat Enterprise Linux Server 6(RPMs)
rhui-REGION-rhel-server-rh-common	Red Hat Enterprise Linux Server 6 RH 공통 (RPMs)
Epel	Enterprise Linux 6용 추가 패키지 - x86_64
pbis	PBIS 패키지 업데이트

- CentOS 7 사전 구성된 리포지토리(일반적으로 5개):

리포지토리 ID	리포지토리 이름
base/7/x86_64	CentOS-7 - 기본
업데이트/7/x86_64	CentOS-7 - 업데이트
extras/7/x86_64	CentOS-7 - 추가 항목

리포지토리 ID	리포지토리 이름
epel/x86_64	Enterprise Linux 7용 추가 패키지 - x86_64
pbis	PBIS 패키지 업데이트

- Microsoft Windows Server의 경우 모든 업데이트는 Windows Update 카탈로그를 사용하도록 구성된 Windows Update Agent를 사용하여 감지되고 설치됩니다(Microsoft Update의 업데이트는 포함되지 않음).

Microsoft Windows 운영 체제에서 패치 관리자는 Microsoft의 cab 파일 wsusscn2.cab을 사용할 수 있는 운영 체제 보안 업데이트의 소스로 사용합니다. 이 파일에는 Microsoft가 게시하는 보안 관련 업데이트에 대한 정보가 포함되어 있습니다. 패치 관리자는 Microsoft에서 이 파일을 정기적으로 다운로드하고 이를 사용하여 Windows 인스턴스에 사용할 수 있는 패치 세트를 업데이트합니다. 파일에는 Microsoft가 보안과 관련된 것으로 식별하는 업데이트만 포함되어 있습니다. 파일의 정보가 처리되면 패치 관리자는 이후 업데이트로 대체된 업데이트도 제거합니다. 그러므로 최신 업데이트만 표시되며 설치 시 사용할 수 있는 상태가 됩니다. 예를 들어 KB4012214가 KB3135456을 대체하는 경우 패치 관리자에서는 KB4012214만 업데이트로 사용할 수 있습니다.

wsusscn2.cab 파일에 대한 자세한 내용은 Microsoft 문서 [Using WUA to Scan for Updates Offline](#)을 참조하세요.

패치 및 인프라 설계

AMS는 인프라 설계에 따라 변경 가능 또는 변경 불가능과 같은 다양한 패치 방법을 사용합니다(자세한 정의는 참조 [AMS 키 용어](#)).

변경 가능한 인프라를 사용하면 AMS 운영 엔지니어가 개별적으로 Amazon EC2 인스턴스에 직접 업데이트를 설치하는 기존 인플레이스 방법론을 사용하여 패치 적용을 수행합니다. 이 패치 방법은 Auto Scaling 그룹이 아닌 스택에 사용되며 단일 Amazon EC2 인스턴스 또는 몇 개의 인스턴스를 포함합니다. 이 시나리오에서는 인스턴스 또는 스택이 기반으로 한 AMI를 교체하면가 완료되지 않도록 처음 배포된 이후 해당 시스템에 대한 모든 변경 사항이 삭제됩니다. 업데이트는 실행 중인 시스템에 적용되며 애플리케이션 또는 시스템 재시작으로 인해 시스템 가동 중지(스택 구성에 따라 다름)가 발생할 수 있습니다. 블루/그린 업데이트 전략을 사용하여 이를 완화할 수 있습니다. 자세한 내용은 [AWS CodeDeploy 블루/그린 배포 소개를 참조하세요](#).

변경 불가능한 인프라의 경우 패치 방법은 AMI 교체입니다. 변경 불가능한 인스턴스는 Auto Scaling 그룹 구성에 지정된 AMI를 대체하는 업데이트된 AMI를 사용하여 균일하게 업데이트됩니다. AMS 릴리

스는 일반적으로 패치 화요일 주인 매월 업데이트(즉, 패치 적용)AMIs. 다음 섹션에서는 작동 방식을 설명합니다.

AMS 표준 패치 적용 방식

AMS는 인프라 배포 전략(변경 가능 또는 변경 불가능)에 따라 현재 위치 및 AMI 교체라는 두 가지 주요 패치 방법과 함께 정기적으로 예약된 월별 및 필요에 따라 중요한 패치에 Systems Manager Run Command 서비스를 사용합니다. 이 섹션에서는 AMS 패치 서비스, 유형, 메서드 및 프로세스에 대해 설명합니다.

AMS는 다르게 예약된 두 가지 패치 유형을 정의합니다.

- 중요 패치 적용: 업데이트는 알림을 수락한 후 최대한 빨리 적용됩니다.
- 표준 패치: 정기적인 OS 공급업체 업데이트 및 월별 적용.

패치는 현재 위치 패치 적용 또는 AMI 교체(요청 시)를 통해 적용됩니다.

스캔 업데이트

AMS는 [Amazon EC2 Run Command Service](#)를 사용하여 Amazon EC2 스택에 연결하고 필요한 스캔 및 패치 스크립트를 배포합니다. AMS는 지원되는 운영 체제에 이미 설치된 기본 패키지 관리 구성 요소를 사용하여 Amazon EC2 스택에서 필요한 모든 스캔 및 패치 작업을 수행합니다. Red Hat 및 Amazon Linux의 경우 서비스는 yum을 사용합니다. Windows의 경우 서비스는 Windows 업데이트 에이전트를 사용합니다.

스캔은 [SSM Maintenance Windows](#) 및 AMS 기본 AWS-RunPatchBaseline 문서를 사용하여 매일 수행됩니다. Linux 및 Windows용 업데이트 리포지토리를 사용하여 도달 가능한 모든 Amazon EC2 스택을 스캔합니다. AMS 패치 프로세스는 도달 가능한 모든 Amazon EC2 스택을 감지한 다음 배치 프로세스에서 스캔을 수행하여 스캔을 실행하는 동안 오류가 발생하더라도 스택이 항상 정상 상태를 유지하도록 합니다. 그런 다음 각 Amazon EC2 스택에 대해 스캔 결과가 저장됩니다.

스택 또는 인스턴스에 대한 스캔 결과를 보려면 스택 ID 또는 인스턴스 ID를 사용하여 서비스 요청을 제출합니다.

기본 AMS 패치 적용 프로세스는 패치 분류 또는 심각도(예: 중요 또는 표준)에 관계없이 사용 가능한 모든 패치를 설치하는 것입니다. 스택에 대해 명시적으로 제외한 패치는 예외입니다(AMS에서 필수로 정의한 패치는 제외해서는 안 됨).

제안된 유지 관리 기간 14일 전에 패치 서비스 알림이 전송됩니다. 이렇게 하면 제안된 패치를 테스트하고 수락하거나 거부할 수 있는 시간이 제공됩니다. 패치 서비스 알림에 응답하지 않으면 인스턴스에

패치가 적용되지 않습니다. 패치를 설치할 시간이 되면 AMS는 각 스택에 대해 변경 요청(RFC)을 생성하고 해당 RFC는 계정의 RFC 목록에 나타납니다.

AMS 구성 유지 관리 기간 및 알림

AMS 구성 패치 적용 시 각 계정에는 계정을 온보딩할 때 정의하는 월별 유지 관리 기간이 있습니다. AWS Managed Services 유지 관리 기간(또는 유지 관리 기간)은 AWS Managed Services(AMS)에 대한 유지 관리 활동을 수행하고 태평양 표준시 기준 매월 두 번째 목요일 오후 3시부터 오후 4시까지 반복됩니다. AMS는 48시간 전에 통지하여 유지 관리 기간을 변경할 수 있습니다.

패치 적용 기간이 다릅니다. 아웃바운드 서비스 패치 요청(서비스 알림이라고도 함)에는 제안된 패치가 포함되어 있습니다.

Note

패치 서비스 알림에 회신하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [AMS 표준 패치에서 수행할 수 있는 작업](#).

패치 서비스 알림은 계정에 등록된 연락처 이메일 주소로 이메일로 전송됩니다. 알림에는 응답할 수 있는 AWS Support 콘솔에 대한 링크가 포함되어 있습니다. AMS 서비스 요청 페이지를 사용하여 알림에 응답할 수도 있습니다. 서비스 알림에는 다음이 포함됩니다.

- 스택에 적용되는 업데이트 IDs(CSUs, IUs 및 OUs) 목록과 요청한 업데이트는 패치 적용에서 제외됩니다(있는 경우).
- 영향을 받을 인스턴스의 IDs.
- 업데이트가 적용될 제안된 패치 기간입니다. 다른 패치 기간을 요청할 수 있습니다.
- 제안된 패치를 수락하거나 추가 정보를 요청하는 요청입니다. AMS는 업데이트의 영향을 테스트하고 패치 적용을 승인 또는 거부하거나 특정 업데이트를 제외하도록 요청할 시간을 제공합니다. 테스트할 시간이 더 필요하고 테스트 후 업데이트를 적용하려면 서비스 알림에 응답하고 원하는 내용을 설명하거나 이전 RFC의 세부 정보를 기반으로 새 패치 RFC에 대한 서비스 요청을 제출합니다. 서비스 알림에 전혀 응답하지 않으면 패치 작업이 수행되지 않고 RFC가 취소됩니다.

서비스 알림을 승인하면 AMS는 패치 RFC를 실행하고 서비스 약정에 따라 합의된 패치 기간 내에 업데이트를 적용합니다.

패치 적용이 완료되면 AMS는 서비스 요청에 패치 적용 활동의 결과(성공 또는 실패)에 대한 요약과 함께 서신을 보냅니다.

인플레이스 패치 적용

현재 위치 패치 적용은 AMS가 각 스택 인스턴스에 로그인하고 패치를 적용하는 방법을 말합니다.

현재 위치 패치는 지원되는 운영 체제를 실행하는 Amazon EC2 인스턴스를 사용하는 변경 가능한 인프라에서 발생합니다. 패치 적용은 해당 시점까지 사용할 수 있는 제외되지 않은 모든 업데이트를 적용합니다. 중요한 패치가 릴리스되면 추가적인 중요한 패치 적용 프로세스가 있습니다.

표준 패치: 인플레이스

표준 패치 적용은 패치 서비스 알림에 제안된 합의된 패치 일정에 따라 수행되며 중요한 것으로 간주되지 않는 정기적인 패치 업데이트를 포함합니다.

제안된 패치 적용 기간 전에 알림에 대한 긍정적인 응답과 함께 패치 RFC가 생성되어 RFC 대시보드에 표시됩니다.

중요 패치 적용: 현재 위치

OS 공급업체가 중요한 보안 업데이트를 릴리스하면 AMS는 AMS 서비스 약정에 따라 각 스택에 대한 서비스 알림(계정의 연락처 이메일)을 보내 패치 RFC를 알립니다. 서비스 알림에는 각 업데이트에 대한 다음이 포함됩니다.

- 릴리스 날짜 업데이트
- 중요도 업데이트
- 세부 정보 업데이트(KB 참조 등)
- 영향을 받는 스택IDs

알림에 나열된 업데이트를 테스트하고 서비스 알림에 회신하여 패치를 승인하거나 거부할 수 있습니다. 알림을 승인하는 경우 업데이트를 설치하기 위해 스택당 특정 패치 기간을 제공해야 합니다.

Note

서비스 알림에 응답한 후 24시간 이내에 있는 패치 기간은 사용 가능한 용량에 따라 다시 예약할 수 있습니다.

10일 이내에 응답하지 않거나 제안된 패치를 거부하면 패치가 취소됩니다.

허용된 기간(알림에 제공됨) 이후에 업데이트를 적용하려면 이전 알림의 세부 정보를 기반으로 새 패치 일정에 대한 서비스 요청을 제출합니다.

서비스 알림을 승인하면 AMS는 서비스 약정에 따라 지정된 패치 기간 내에 업데이트를 적용합니다.

여러 업데이트의 경우 서비스 알림에 대한 응답에서 제외할 업데이트를 지정하여 패치 적용에서 특정 업데이트를 제외할 수 있습니다.

AMS는 각 스택에 대해 각 업데이트의 결과(즉, 성공 또는 실패)에 대한 서비스 알림을 보냅니다.

AMI 업데이트 패치 적용(Auto Scaling 그룹에 패치된 AMIs 사용)

AMI 교체 패치는 Auto Scaling 그룹에 새 Amazon EC2 인스턴스를 배포하도록 구성된 AMI ID를 업데이트하여 변경 불가능한 인프라에서 수행됩니다.

Amazon Machine Image(AMIs)는 지원되는 운영 체제에 대해 정기적으로 릴리스됩니다. 운영 체제 공급업체는 정기적으로 새 패치를 릴리스합니다. AMS는 Amazon에서 제공하는 AMI를 가져와 최신 패치로 업데이트한 다음 적절한 구성 요소를 추가하여 AMS 환경에서 작동할 수 있도록 합니다. 그런 다음 계정에 AMI를 공유하여 모든 AMS 고객이 새 AMS AMI를 사용할 수 있도록 합니다. Auto Scaling 그룹 스택은 새로 릴리스된 AMS AMIs. 다음 그림은 AMS 환경에서 AMIs 사용하는 방법을 보여줍니다.

Auto Scaling 그룹은 Auto Scaling 그룹에 대해 구성된 AMI를 기반으로 인스턴스를 생성합니다. AMS가 업데이트된 AMIs 공유하는 경우 AMI 업데이트를 관리하는 방법에 따라 다음과 같은 옵션이 있습니다.

- 인스턴스가 생성된 후 자동으로 사용자 지정하는 애플리케이션 배포 도구(예: UserData, CodeDeploy 등)를 사용하는 경우 다음을 수행할 수 있습니다.
 - 패치 서비스 알림에 회신하거나 최신 AMS AMI에 대한 서비스 요청을 제출하여 현재 Auto Scaling 그룹의 구성 AMI를 교체합니다. Auto Scaling 그룹 구성의 AMI ID가 교체되면 AMS는 인스턴스의 롤링 업데이트를 시작하고 Auto Scaling 그룹 인스턴스 구성(예: 애플리케이션 설치, 스크립트 부팅 등)은 새 AMS AMI로 생성된 새 인스턴스에 자동으로 적용됩니다.
- Auto Scaling 그룹의 구성에서 사용자 지정/골든 AMI를 사용하는 경우 다음을 수행할 수 있습니다.
 - 새 AMS AMI를 사용하여 인스턴스를 생성하고, 인스턴스를 사용자 지정하고, 새 골든 AMI를 생성합니다. Amazon EC2 콘솔을 사용하여 새 골든 AMI를 AMS와 공유하고 AMS에 서비스 요청을 제출하여 새 사용자 지정 AMI를 사용하도록 Auto Scaling 그룹의 구성을 업데이트합니다.
 - Amazon EC2 콘솔을 사용하여 기존 골든 AMI를 AMS와 공유하고 AMS에 대한 서비스 요청을 제출하여 골든 AMI를 업데이트합니다. 이를 위해 AMS는 골든 AMI에서 인스턴스를 생성하고, 해당 인스턴스에 패치를 적용하고, 사용자를 위해 새 골든 AMI를 생성한 다음 새 AMI를 사용하도록 Auto Scaling 그룹의 구성을 업데이트합니다. 단점은 AMS가 새 사용자 지정 AMI가 원하는 방식으로 작동하는지 테스트할 수 없다는 것입니다. 대신 새 골든 AMI를 생성하고 공유하며 AMS가 Auto

Scaling 그룹을 업데이트하도록 요청하기 전에 새 AMI로 생성된 인스턴스를 테스트하고 모든 것이 올바르게 작동하는지 확인해야 합니다. AMS는 이 옵션을 권장하지 않습니다.

표준 패치: AMI 업데이트

매달 AMS는 서비스 개선 사항과 AMIs에 적용되는 새로운 패치가 포함된 새로운 Amazon Machine Image(AMIs).

Note

업데이트된 AWS AMIs에서 패치 화요일 이후에 새 AMS AMIs 생성됩니다. 그런 다음 AMS는 사용 가능하게 만들기 전에 테스트합니다. 새 AMIs가 테스트를 통과하면 AMSAMIs를 관리형 계정에 공유합니다.

중요 패치: AMI 업데이트

필요한 경우 AMS는 지난 달 AMIs 릴리스 이후 릴리스된 중요한 보안 패치로 업데이트된 AMI를 제공합니다.

변경 불가능한 인프라에 대한 중요 보안 업데이트 프로세스는 변경 불가능한 인프라에 대한 월별 AMI 프로세스와 동일합니다. 단, 새로운 중요 업데이트 릴리스에 따라 정상적인 일정(패치 화요일)을 벗어나 새 AMS AMI가 생성됩니다. AMS는 계정에 정의된 서비스 수준 계약(SLAs)에 따라 중요한 보안 패치가 있는 새 AMI를 제공합니다. 요청별 Auto Scaling 그룹의 AMS 업데이트만 가능합니다. 서비스 요청을 사용하여 AMI 교체 요청을 제출합니다.

AMS 표준 패치 적용 실패

업데이트가 실패할 경우 AMS는 분석을 수행하여 실패 원인을 이해하고 분석 결과를 사용자에게 전달합니다. 장애가 AMS에 기인하는 경우 유지 관리 기간 내에 있는 경우 업데이트를 다시 시도합니다. 그렇지 않으면 AMS는 실패한 인스턴스 업데이트에 대한 서비스 알림을 생성하고 지침을 기다립니다.

시스템에서 발생하는 장애의 경우 새 패치 RFC로 서비스 요청을 제출하여 인스턴스를 업데이트할 수 있습니다.

AMS 표준 패치에서 수행할 수 있는 작업

새 AMIs를 테스트하는 것 외에도 인프라의 패치를 관리하기 위해 취할 수 있는 몇 가지 조치가 있습니다.

- 업데이트를 테스트하는 데 허용된 패치 기간보다 오래 걸린 경우 서비스 요청을 제출하여 AMS에 준비가 되었을 때 취소된 업데이트를 적용하도록 요청할 수 있습니다(원본 서비스 알림의 세부 정보를 기반으로 사용).
- 업데이트 목록, 해당 인스턴스 및 기타 세부 정보를 제공하는 서비스 요청을 제출하여 다음 자동 업데이트 기간 전에 중요 업데이트(IU) 또는 기타 업데이트(OU)를 적용하도록 요청할 수 있습니다. 이 CT는 자동화되지 않으므로 예약 및 실행 시간이 더 오래 걸립니다. 적절한 시간 동안 서비스 수준 목표(SLOs)를 확인합니다. 자세한 내용은 [AMS 서비스 수준 목표\(SLOs\)](#) 단원을 참조하십시오.

또한 패치가 적용된 기존 AMS AMIs 사용하여 사용자 지정 AMIs. 자세한 내용은 [AMI | 생성](#)을 참조하세요.

Note

AMS AMI 릴리스 프로세스는 모든 AMS 고객의 이익을 위해 균일한 주기를 따르기 때문에 다음 유지 관리 기간 전에 중요한 업데이트 또는 기타 업데이트를 기반으로 새 AMS AMI를 요청할 수 없습니다.

패치되는 항목 변경/옵트아웃

AMS 구성 패치를 사용하면 패치 서비스 알림 또는 서비스 요청에 대한 응답으로 패치할 리소스를 변경할 수 있습니다. 다음을 수행할 수 있습니다.

- 문제 해결에서 제외해야 하는 패치 목록을 스택별 및 운영 체제별로 정의합니다.
- 특정 패치 또는 모든 패치에서 제외해야 하는 리소스 목록을 정의합니다.
- 모든 패치 적용에서 항상 제외해야 하는 리소스 목록을 정의합니다.
- 특정 날짜 및 특정 시간에 패치해야 하는 리소스 목록을 정의합니다(유지 관리 기간을 정의하지 않은 경우 양호).

하나 이상의 패치를 제외하려면 서비스 요청을 제출하거나 다음에 제공된 템플릿을 사용하여 패치 서비스 알림에 응답합니다. RFC를 제출하지 마십시오. 제외하려는 패치 이름과 이유를 요청에 포함합니다. 다음과 같이 서비스 요청에 이 정보를 포함합니다.

- 이름: 패치의 이름입니다. Windows 패치의 경우와 같은 KB 이름입니다 KB3145384. Linux 패치의 경우와 같은 패키지 이름입니다 openssh-6.6.1p1-25.61.amzn1.x86_64.
- 이유: 패치가 제외되는 이유를 나타내는 설명입니다.

- 만료 시간: 제외가 만료되는 날짜/시간입니다.

제외된 패치가 이미 설치된 경우 제거됩니다.

이러한 패치를 제외하면 심각한 보안 위험이 발생할 경우 운영자가 요청을 검토합니다. 제외된 패치의 만료 날짜도 협상됩니다. 합의된 만료 날짜가 지나면 제외가 만료되고 패치가 후속 패치에 설치됩니다.

해당하는 경우 제외 목록의 패치는 스캔 결과에 계속 반환됩니다.

Note

Windows와 달리 Linux 패치는 버전별로 다릅니다. 제외된 패치의 새 버전은 자동으로 제외되지 않으므로 이러한 구분이 중요합니다. 원하는 경우 새 버전의 Linux 패치를 제외하도록 AMS에 알리는 것은 사용자의 책임입니다.

패치 서비스 알림 응답 템플릿

인스턴스에서 패치를 수행하려면 지정된 형식을 사용하여 패치 서비스 알림에 응답해야 합니다. AMS로 유지 관리 기간을 아직 설정하지 않은 경우 이 작업을 수행해야 합니다.

서비스 알림에 회신할 때 지정된 형식을 사용합니다.

유지 관리 기간이 설정되지 않은 경우 다음과 같이 패치할 시기를 알려주십시오.

UTC	StartTime	StackId	InstanceId (Optional)
2019-04-01	15:00	stack-123456789012	i-1234566789
2019-04-01	15:00	stack-123456789013	i-1234566784
2019-04-01	15:00	stack-123456789014	i-1234566783
2019-04-01	15:00	stack-123456789015	i-1234566782

유지 관리 기간이 설정되어 있고 특정 리소스가 특정 패치에서 제외되도록 하려면 다음 형식을 사용합니다.

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	<i>PATCH</i>
stack-123456789013	i-1234566784	<i>PATCH</i>
stack-123456789014	i-1234566783	<i>PATCH</i>
stack-123456789015	i-1234566782	<i>PATCH</i>

유지 관리 기간이 설정되어 있고 특정 리소스가 항상 모든 패치에서 제외되도록 하려면 다음 형식을 사용합니다.

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	ALL
stack-123456789015	i-1234566782	ALL

패치 준비

자동 패치 적용을 위해 환경을 준비하려면 다음을 수행하는 것이 좋습니다.

- 패치할 모든 인스턴스의 전체 인벤토리가 있는지 확인합니다.
- 비즈니스 연속성 전략의 일환으로 리소스를 정기적으로 백업해야 합니다. 추가 백업은 패치 시퀀스의 일부로 생성되며 구성된 패치 오케스트레이터 보존 정책에 따라 자동으로 삭제됩니다(기본값은 60일).
- 모든 관련 라이선스가 최신 상태인지 확인합니다.
- 테스트 스택이 프로덕션 스택보다 먼저 패치되도록 스택 유지 관리 기간을 수정하여 패치 적용에 시차를 둡니다. 이렇게 하면 패치 적용과 관련된 모든 오류가 테스트 스택에서 발견되며 프로덕션 스택이 패치되기 전에 식별할 수 있습니다.

패치 설정 보기

현재 패치 구성이 무엇인지 확인하려면 다음을 수행할 수 있습니다.

- 쿼리를 사용하여 AMS에 서비스 요청을 제출합니다.
- 패치 서비스 알림을 기다립니다. 패치 적용 알림은 적용할 모든 패치와 패치할 인스턴스를 알려주고 패치 기간도 제안합니다.

서비스 요청을 제출하여 다음을 수정할 수 있습니다.

- 스캔 간격: 이 스택의 인스턴스에 대해 수행된 규정 준수 스캔 사이의 시간입니다.

기본값은 240 (4시간)입니다.

- NotificationWindow: 예약된 변경(패치)의 사전(분) 알림을 보내야 하는 시간입니다. 기본값은 10080 (7일)입니다.

AMS 표준 패치 FAQs

이 섹션에서는 몇 가지 자주 묻는 질문에 대한 답변을 제공합니다.

- Q: 글로벌 패치 적용을 옵트아웃하려면 어떻게 해야 하나요?

A: 패치 적용을 전역적으로 옵트아웃하려면 서비스 요청을 제출합니다. AMS 필수 패치는 옵트아웃할 수 없습니다. 취약성을 보고할 수 있도록 모든 스택은 계속 스캔됩니다.

- Q: 패치 적용에서 특정 스택을 제외하려면 어떻게 해야 합니까?

A: 패치 적용에서 특정 스택을 영구적으로 제외하려면 서비스 요청을 제출합니다. 특정 패치 주기에서 특정 스택을 제외하려면 제외할 스택 목록과 함께 예정된 패치 적용 알림에 응답합니다. 자세한 내용은 [패치되는 항목 변경/옵트아웃](#) 단원을 참조하세요. 필수 패치는 옵트아웃할 수 없습니다.

- Q: 패치 서비스 알림을 승인하지 않으면 어떻게 되나요?

A: 표준 패치 적용 서비스 요청을 승인할 수 있는 기간은 14일이고 중요한 패치 적용 공지를 승인할 수 있는 기간은 10일입니다. 기간 내에 서비스 요청을 승인하지 않으면 서비스 커밋이 무효화되고 패치가 발생하지 않습니다. 필수 패치 적용의 경우 서비스 요청에 대한 응답과 관계없이 패치가 적용됩니다.

- Q: 특정 패치 및 패키지가 설치되지 않도록 제외하려면 어떻게 해야 합니까?

A: 특정 패치 또는 패키지를 영구적으로 제외하려면 서비스 요청을 제출합니다. 특정 패치 주기에서 특정 패치 또는 패키지를 제외하려면 제외할 패치 또는 패키지 목록으로 예정된 패치 적용 알림에 응답합니다. 자세한 내용은 [패치되는 항목 변경/옵트아웃](#)을 참조하세요. 필수 패치는 옵트아웃할 수 없습니다.

- Q: 패치 적용으로 인해 시스템에 장애가 발생하면 어떻게 되나요?

A: AMS는 각 시스템을 모니터링합니다. AMS는 스택 및 인스턴스당 각 업데이트의 결과(즉, 성공 또는 실패)에 대한 서비스 알림을 보냅니다. 장애가 감지되면 AMS는 인스턴스를 조사하고 복원하는 작업을 수행한 다음 AMS 작업 엔지니어가 수동으로 패치를 시도합니다. 자세한 내용은 [AMS 표준 패치 적용 실패](#) 단원을 참조하세요.

- Q: AMS에서 관리하는 업데이트는 무엇입니까?

A: AMS는 공급업체가 AMS에 알리는 운영 체제 수준 업데이트를 관리합니다. 자세한 내용은 [지원되는 패치](#) 단원을 참조하십시오.

- Q: AMS에서 관리하지 않는 업데이트는 무엇입니까?

A: 애플리케이션 수준 업데이트는 AMS에서 관리하지 않습니다.

- Q: Auto Scaling 그룹은 어떻게 업데이트되나요?

A: Auto Scaling 그룹은 Auto Scaling 그룹 구성에서 AMI 교체로 업데이트되고 롤링 업데이트를 미리 구성합니다. 롤링 업데이트는 패치 구성의 HealthyHostThreshold 설정을 관찰하여 패치 적용 중에 스택의 Amazon EC2 인스턴스 수를 활성 상태로 유지해야 합니다. 자세한 내용은 [AMI 업데이트 패치 적용\(Auto Scaling 그룹에 패치된 AMIs 사용\)](#) 단원을 참조하십시오.

- Q: 정상 주기 외에 업데이트를 설치하려면 어떻게 해야 하나요?

A: 일반 패치 적용 일정을 벗어나 설치하려는 OS 수준 업데이트의 경우 수신한 패치 적용 알림을 사용하여 서비스 요청을 제출합니다. 이는 제안된 패치 테스트에 21일(표준 패치의 경우) 또는 14일(중요 패치의 경우)이 넘게 걸린 경우 발생할 수 있습니다. 독립 실행형 Amazon EC2 인스턴스의 경우 Out-of-band 패치 적용을 현재 위치에서 수행할 수 있습니다.

- Q: 새로 배포된 스택 또는 인스턴스는 어떻게 패치되나요?

A: 새 Amazon EC2 스택 인스턴스 또는 Auto Scaling 그룹을 생성할 때는 항상 최신 패치가 이미 있는 최신 AMS AMI를 지정해야 합니다. 변경 가능한 인프라의 경우 스택이 배포되는 즉시 인라인 패치 적용을 수행해야 합니다.

서비스 커밋 패치 적용

인프라 배포 유형과 업데이트의 중요도에 따라 변경 및 변경 불가능한 인프라에 대한 중요한 보안 업데이트와 변경 및 변경 불가능한 인프라에 대한 중요한 업데이트에 대한 서비스 약정을 제공합니다.

표준 패치 적용

표준 패치를 위한 AMS 서비스 약정입니다.

표준 패치 적용, 변경 가능한 인프라(인플레이스 패치 적용)

이벤트/작업	서비스 약정 측정
중요 업데이트는 한 달에 릴리스됩니다.	클럭 시작
표준 패치 알림이 생성된 후 14일이 지나면 AMS는 서비스 알림과 각 스택에 대한 이메일을 통해 예정된 패치 적용을 알립니다. 서비스 알림에는 다음이 포함됩니다. - 스택에 적용 가능한(필수 및 적용되지 않은) 업데이트 IDs(CSUs 및 IUs) 및 패치 적용에서 제외된 업데이트 목록 - 영향을 받는 스택IDs - 업데이트가 적용될 유지 관리 기간	서비스 알림이 전송된 후 시계가 중지됩니다.
업데이트의 영향을 테스트하고 RFC를 승인하거나 거부합니다. 14일 이내에 응답하지 않거나 서비스 알림에 대한 응답에서 패치 적용을 거부하면 아무 조치도 취하지 않습니다.	14일 이내에 승인하거나 회신하지 않으면 보류 중인 변경 사항이 취소되고 업데이트에 대한 서비스 약정이 적용되지 않습니다.
테스트하는 데 14일이 넘게 걸리고 14일 후에 업데이트를 적용하려면 이전 RFC의 세부 정보를 기반으로 새 패치 RFC에 대한 서비스 요청을 제출합니다.	
14일 이내에 서비스 알림을 승인하면 AMS가 업데이트를 적용합니다.	수신 후 14일 이내에 서비스 알림을 승인하면 시계가 시작됩니다. 업데이트 설치를 시도한 후 시계가 중지됩니다.

이벤트/작업	서비스 약정 측정
서비스 알림에 대한 응답에서 제외할 업데이트를 지정하여 RFC에서 특정 업데이트를 제외하도록 선택할 수 있습니다.	
AMS는 시도된 각 업데이트의 결과에 대한 서비스 알림을 보냅니다. 서비스 알림에는 다음 세부 정보가 포함됩니다. • Amazon EC2 인스턴스 ID • 업데이트 1 성공/실패: ARN a1, ARN a2... • 업데이트 2 성공/실패: ARN b1, ARN b2... • N 업데이트 성공/실패: ARN c1, ARN c2...	해당 사항 없음.
업데이트가 실패할 경우 AMS는 분석을 수행하여 실패 원인을 이해하고 분석 결과를 사용자에게 전달합니다. 장애가 AMS에 기인하는 경우 AMS는 유지 관리 기간 내에 업데이트를 재시도합니다. 그렇지 않으면 AMS는 실패한 인스턴스 업데이트 조합에 대한 서비스 알림을 생성하고 유지 관리 기간에 대한 지침을 기다립니다.	해당 사항 없음.
장애가 발생한 경우 새 패치 RFC에 대한 서비스 요청을 제출하여 인스턴스를 업데이트합니다.	해당 사항 없음.

중요 패치 적용

다음은 중요한 보안 업데이트를 위한 AMS 서비스 약정입니다.

중요한 보안 업데이트, 변경 가능한 인프라

이벤트/작업	서비스 약정 측정
CSU가 릴리스되었습니다.	클럭 시작

이벤트/작업	서비스 약정 측정
AMS는 각 스택에 대한 서비스 알림(이메일도 전송)을 통해 패치 RFC를 알립니다. 서비스 알림에는 다음이 포함됩니다. • 릴리스 날짜 업데이트 • 중요도 업데이트 • 업데이트 세부 정보: KB 참조 등 • 영향을 받는 스택IDs	서비스 알림이 전송된 후 시계가 중지됩니다.
RFC에 나열된 업데이트를 테스트하고 서비스 알림에 회신하여 10일 이내에 RFC를 승인하거나 거부합니다. 업데이트를 설치하기 위한 특정 유지 관리 기간(스택당)을 제공합니다. 서비스 알림에 응답한 후 24시간 이내에 지정된 유지 관리 기간은 사용 가능한 용량에 따라 다시 예약할 수 있습니다. 10일 이내에 응답하지 않거나 패치 RFC를 거부하면 보류 중인 작업이 취소됩니다. 14일 기간 이후에 업데이트를 적용하려면 이전 RFC의 세부 정보를 기반으로 새 패치 RFC에 대한 서비스 요청을 제출합니다.	14일 이내에 승인하거나 회신하지 않으면 보류 중인 변경 사항이 취소되고 업데이트에 대한 서비스 약정이 적용되지 않습니다.
서비스 알림을 승인하면 AMS가 업데이트를 적용합니다. 여러 업데이트의 경우 서비스 알림에 대한 응답에서 제외할 업데이트를 지정하여 변경에서 특정 업데이트를 제외하도록 선택할 수 있습니다.	원하는 유지 관리 기간이 서비스 약정 기간 내에 있지 않으면 RFC가 원하는 유지 관리 기간 내에 실행되지 않는 경우에만 업데이트에 대한 서비스 약정이 누락됩니다.

이벤트/작업	서비스 약정 측정
AMS는 적용된 각 업데이트의 결과에 대한 서비스 알림을 보냅니다. 서비스 알림에는 다음 세부 정보가 포함됩니다. - Amazon EC2 인스턴스 ID - 업데이트 성공: ARN a1, ARN a2... - 업데이트 실패: ARN c1, ARN c2...	해당 사항 없음.
업데이트가 실패할 경우 AMS는 분석을 수행하여 실패 원인을 이해하고 분석 결과를 사용자에게 전달합니다. 장애가 AMS에 기인하는 경우 AMS는 유지 관리 기간 내에 업데이트를 재시도합니다. 그렇지 않으면 AMS는 실패한 인스턴스 업데이트 조합에 대한 서비스 알림을 생성하고 새 유지 관리 기간에 대한 지침을 기다립니다.	해당 사항 없음.
장애가 발생한 경우 새 패치 RFC에 대한 서비스 요청을 제출하여 인스턴스를 업데이트합니다.	해당 사항 없음.

중요한 보안 업데이트, 변경 불가능한 인프라

이벤트/작업	서비스 약정 측정
CSU가 릴리스되었습니다.	클럭 시작
AMS는 서비스 알림을 통해 다음을 알립니다. - 릴리스 날짜 업데이트 - 중요도 업데이트 - 세부 정보 업데이트(KB 참조 등) - 영향을 받는 AMS Amazon Machine Image(AMI) - 업데이트된 새 AMIs의 예상 릴리스 날짜 및 시간	클럭은 계속 실행됩니다.

이벤트/작업	서비스 약정 측정
AMS는 관리형 계정에서 업데이트된 AMIs.	시계가 중지됩니다.
서비스 알림을 승인하면 AMS가 업데이트를 적용합니다. AMS는 서비스 알림 및 이메일을 통해 계정에서 공유된 AMIs를 사용자에게 알립니다.	해당 사항 없음.
새 AMIs를 테스트하는 데 할당된 시간(1주)보다 오래 걸리는 경우 AMS에 서비스 요청을 제출하여 Auto Scaling 그룹을 새 AMS AMI(있는 그대로)로 업데이트할 수 있습니다. 구성으로 새 AMS AMI를 수정하려면 관리 기타 기타 CT 업데이트(ct-0xdawir96cy7k)와 함께 RFC를 사용하여 Auto Scaling 그룹 업데이트를 요청합니다.	해당 사항 없음.

보고서 및 옵션

AWS Managed Services(AMS)는 다양한 네이티브 AWS 서비스의 데이터를 수집하여 주요 AMS 제품에 대한 부가가치 보고서를 제공합니다.

AMS는 두 가지 유형의 세부 보고를 제공합니다.

- **요청 보고서:** Cloud Service Delivery Manager(CSDM)를 통해 특정 보고서를 임시로 요청할 수 있습니다. 온보딩 또는 중요한 이벤트 중에 보고서를 여러 번 요청해야 할 수 있으므로 이러한 보고서에는 제한이 없습니다. 그러나 이러한 보고서는 주간 보고서와 같은 일정에 따라 제공되도록 설계되지 않았습니다. 요구 사항을 더 잘 이해하거나 셀프 서비스 보고 사용에 대한 자세한 내용은 CSDM에 문의하십시오.
- **셀프 서비스 보고서:** AMS 셀프 서비스 보고서를 사용하면 필요한 만큼 자주 데이터를 직접 쿼리하고 분석할 수 있습니다. 셀프 서비스 보고서를 사용하여 AMS 콘솔에서 보고서에 액세스하고 S3 버킷(계정당 버킷 1개)을 통해 데이터 세트를 보고합니다. 이를 통해 원하는 비즈니스 인텔리전스(BI) 도구에 데이터를 통합하여 요구 사항에 맞게 보고서를 사용자 지정할 수 있습니다.

주제

- [요청 시 보고서](#)
- [셀프 서비스 보고서](#)

요청 시 보고서

주제

- [AMS 패치 보고서](#)
- [AMS 백업 보고서](#)
- [인시던트 방지 및 상위 화자 보고서 모니터링](#)
- [결제 요금 세부 정보 보고서](#)
- [신뢰할 수 있는 수정자 보고서](#)

AMS는 다양한 네이티브 AWS 서비스의 데이터를 수집하여 주요 AMS 제품에 대한 부가가치 보고서를 제공합니다. 이러한 보고서의 사본을 보려면 Cloud Service Delivery Manager(CSDM)에 요청합니다.

AMS 패치 보고서

사용 가능한 보고서

- [패치 인스턴스 세부 정보 요약 보고서](#)
- [패치 세부 정보 보고서](#)
- [패치가 누락된 인스턴스 보고서](#)
- [SSM 적용 범위 보고서 패치 적용](#)

패치 인스턴스 세부 정보 요약 보고서

패치 인스턴스 세부 정보 요약 보고서는 보고에 온보딩된 인스턴스에 대해 수집된 인스턴스 세부 정보를 제공합니다. 이는 온보딩된 모든 인스턴스, 계정 상태, 인스턴스 세부 정보, 유지 관리 기간 적용 범위, 유지 관리 기간 실행 시간, 스택 세부 정보 및 플랫폼 유형을 식별하는 데 도움이 되는 정보 보고서입니다. 이 보고서는 다음을 제공합니다.

1. 계정의 프로덕션 및 비프로덕션 인스턴스에 대한 데이터입니다. 참고: 프로덕션 및 비프로덕션 단계는 인스턴스 태그가 아닌 계정 이름에서 파생됩니다.
2. 플랫폼 유형별 인스턴스 배포에 대한 데이터입니다. 참고: 'N/A' 플랫폼 유형은가 플랫폼 정보를 검색할 수 없는 경우 AWS Systems Manager입니다.
3. 인스턴스의 상태 분포 및 실행, 중지 또는 종료되는 인스턴스 수에 대한 데이터입니다.

필드 이름	정의
보고서 날짜/시간	보고서가 생성된 날짜와 시간입니다.
계정 ID	인스턴스 ID가 속한 AWS 계정 ID
계정 이름	AWS 계정 이름
프로덕션 계정	계정 이름에 'PROD', 'NONPROD' 값이 포함되는지 여부에 따라 AMS prod, 비prod 계정의 식별자입니다. 예: PROD, NONPROD, Not Available
계정 상태	AMS 계정 상태. 예: ACTIVE, INACTIVE

필드 이름	정의
AMS 계정 서비스 약정	우측성, 우측성
랜딩 존	계정 랜딩 존 유형에 대한 플래그입니다. 예: MALZ, NON-MALZ
액세스 제한	액세스가 제한된 리전. 예: US SOIL
인스턴스 ID	EC2 인스턴스의 ID
인스턴스 이름	EC2 인스턴스의 이름
인스턴스 플랫폼 유형	운영 체제(OS) 유형입니다. 예: Windows, Linux 등
인스턴스 플랫폼 이름	운영 체제(OS) 이름입니다. 예: Microsoft WindowsServer2012R2Standard, RedHatEnterpriseLinuxServer
[Stack Name]	인스턴스가 포함된 스택의 이름
스택 유형	AMS 스택(고객 계정 내 AMS 인프라) 또는 고객 스택(고객 애플리케이션을 지원하는 AMS 관리형 인프라). 예: AMS, CUSTOMER
오토 스케일링 그룹 이름	인스턴스가 포함된 Auto Scaling 그룹(ASG)의 이름
인스턴스 패치 그룹	인스턴스를 그룹화하고 동일한 유지 관리 기간을 적용하는 데 사용되는 패치 그룹 이름입니다. 패치 그룹이 할당되지 않은 경우 값은 "Unassigned"가 됩니다.

필드 이름	정의
인스턴스 패치 그룹 유형	패치 그룹 유형입니다. DEFAULT: 인스턴스의 AMSDefaultPatchGroup:True 태그에 의해 결정되는 기본 유지 관리 기간이 있는 기본 패치 그룹입니다. CUSTOMER: 고객이 패치 그룹을 생성했습니다. NOT_ASSIGNED: 패치 그룹이 할당되지 않음
인스턴스 상태	EC2 인스턴스 수명 주기 내의 상태입니다. 예: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING. 자세한 내용은 인스턴스 수명 주기를 참조하세요.
유지 관리 기간 범위	이 인스턴스에 향후 유지 관리 기간이 있는 경우. 예: coveredED 또는 NOT_COVERED
유지 관리 기간 실행 날짜/시간	다음에 유지 관리 기간이 실행될 것으로 예상되는 경우 NULL인 경우 단일 창 실행, 즉 반복되지 않음

패치 세부 정보 보고서

AWS Managed Services(AMS) 패치 세부 정보 보고서는 다음을 포함한 다양한 인스턴스의 패치 세부 정보 및 유지 관리 기간 범위를 제공합니다.

1. 패치 그룹 및 해당 유형에 대한 데이터입니다.
2. 유지 관리 기간, 기간, 마감, 향후 유지 관리 기간 실행 날짜(일정) 및 각 기간의 영향을 받는 인스턴스에 대한 데이터입니다.
3. 계정의 모든 운영 체제에 대한 데이터 및 운영 체제가 설치된 인스턴스 수입니다.

필드 이름	정의
보고서 날짜/시간	보고서가 생성된 날짜와 시간입니다.
계정 ID	인스턴스 ID가 속한 AWS 계정 ID
계정 이름	AWS 계정 이름
인스턴스 ID	EC2 인스턴스의 ID
프로덕션 계정	계정 이름에 'PROD', 'NONPROD' 값이 포함되는지 여부에 따라 AMS prod, 비prod 계정의 식별자입니다. 데이터를 사용할 수 없는 경우 값은 "사용할 수 없음"이 됩니다.
계정 상태	AMS 계정 상태. 예: ACTIVE, INACTIVE
인스턴스 플랫폼 유형	운영 체제(OS) 유형입니다. 예: Windows, Linux
인스턴스 플랫폼 이름	운영 체제(OS) 이름입니다. 예: Microsoft WindowsServer2012R2Standard, RedHatEnterpriseLinuxServer
스택 유형	AMS 스택(고객 계정 내 AMS 인프라) 또는 고객 스택(고객 애플리케이션을 지원하는 AMS 관리형 인프라). 예: AMS, CUSTOMER
인스턴스 패치 그룹	인스턴스를 그룹화하고 동일한 유지 관리 기간을 적용하는 데 사용되는 패치 그룹 이름입니다. 패치 그룹이 할당되지 않은 경우 값은 "Unassigned"가 됩니다.
인스턴스 패치 그룹 유형	패치 그룹 유형입니다. DEFAULT: 인스턴스의 AMSDefaultPatchGroup:True 태그로 결정되는 기본 유지 관리 기간이 있는 기본 패치 그룹 고객: 고객이 생성한 패치 그룹

필드 이름	정의
	UNASSIGNED: 패치 그룹이 할당되지 않음
인스턴스 상태	EC2 인스턴스 수명 주기 내의 상태입니다. 예: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING 자세한 내용은 인스턴스 수명 주기를 참조하세요 .
유지 관리 기간 ID	유지 관리 기간 식별자
유지 관리 기간 상태	가능한 값은 ENABLED 또는 DISABLED입니다.
유지 관리 기간 유형	유지 관리 기간 유형
유지 관리 기간 다음 실행 날짜/시간	다음에 유지 관리 기간이 실행될 것으로 예상되는 경우 NULL인 경우 단일 창 실행, 즉 반복되지 않음
마지막 실행 유지 관리 기간	유지 관리 기간이 실행된 최근 시간
유지 관리 기간(시간)	유지 관리 기간의 지속 시간
유지 관리 기간 적용 범위	유지 관리 기간 적용 범위
패치 기준 ID	현재 인스턴스에 연결된 패치 기준
패치 상태	전체 패치 규정 준수 상태입니다. 예: COMPLIANT, NON_COMPLIANT. 누락된 패치가 하나 이상 있는 경우 인스턴스는 규정을 준수하지 않는 것으로 간주되고, 그렇지 않으면 규정을 준수하는 것으로 간주됩니다.
규정 준수 - 합계	규정 준수 패치 수(모든 심각도)
규정 미준수 - 합계	규정 미준수 패치 수(모든 심각도)
규정 준수 - 중요	심각도가 "중요"인 규정 준수 패치 수

필드 이름	정의
규정 준수 - 높음	심각도가 "높음"인 규정 준수 패치 수
규정 준수 - 중간	심각도가 "중간"인 규정 준수 패치 수
규정 준수 - 낮음	심각도가 "낮음"인 규정 준수 패치 수
규정 준수 - 정보 제공	"정보" 심각도의 규정 준수 패치 수
규정 준수 - 지정되지 않음	심각도가 "지정되지 않음"인 규정 준수 패치 수
규정 미준수 - 중요	심각도가 "중요"인 규정 미준수 패치 수
규정 미준수 - 높음	심각도가 "높음"인 규정 미준수 패치 수
규정 미준수 - 중간	심각도가 "중간"인 규정 미준수 패치 수
규정 미준수 - 낮음	심각도가 "낮음"인 규정 미준수 패치 수
규정 미준수 - 정보 제공	심각도가 "정보"인 규정 미준수 패치 수
규정 미준수 - 지정되지 않음	심각도가 "지정되지 않음"인 규정 미준수 패치 수

패치가 누락된 인스턴스 보고서

패치가 누락된 AWS Managed Services(AMS) 인스턴스 보고서는 다음을 포함하여 마지막 유지 관리 기간 실행 중에 패치가 누락된 인스턴스에 대한 세부 정보를 제공합니다.

1. 패치 ID 수준에서 누락된 패치에 대한 데이터입니다.
2. 패치 심각도, 패치되지 않은 일수, 범위 및 패치 릴리스 날짜와 같은 속성과 함께 하나 이상의 패치가 누락된 모든 인스턴스의 데이터입니다.

필드 이름	정의
보고서 날짜/시간	보고서가 생성된 날짜와 시간입니다.
계정 ID	인스턴스 ID가 속한 AWS 계정 ID

필드 이름	정의
계정 이름	AWS 계정 이름
프로덕션 계정	계정 이름에 'PROD','NONPROD' 값이 포함되어 있는지 여부에 따라 AMS prod, 비prod 계정의 식별자입니다.
계정 상태	AMS 계정 상태. 예: ACTIVE 또는 INACTIVE
AMS 계정 서비스 계층	우측성 또는 우측성
인스턴스 ID	EC2 인스턴스의 ID
인스턴스 플랫폼 유형	운영 체제(OS) 유형입니다. 예: Windows
인스턴스 상태	EC2 인스턴스 수명 주기의 상태입니다. 예: TERMINATED, RUNNING, STOPPING, STOPPED, SHUTTING-DOWN, PENDING 자세한 내용은 인스턴스 수명 주기를 참조하세요 .
패치 ID	릴리스된 패치의 ID입니다. 예: KB3172729
패치 심각도	게시자당 패치 심각도입니다. 예: CRITICAL, IMPORTANT, MODERATE, LOW, UNSPECIFIED
패치 분류	게시자당 패치 분류. 예: CRITICALUPDATES, SECURITYUPDATES, UPDATEROLLUPS, UPDATES, FEATUREPACKS
패치 릴리스 날짜/시간(UTC)	게시자당 패치 릴리스 날짜
패치 설치 상태	SSM당 인스턴스에 패치 상태를 설치합니다. 예: INSTALLED, MISSING, NOT applicable
패치되지 않은 일수	마지막 SSM 스캔 이후 인스턴스의 패치가 해제된 일수

필드 이름	정의
패치되지 않은 일수 범위	패치되지 않은 일수의 버킷팅입니다. 예: <30일, 30~60일, 60~90일, 90일 이상

SSM 적용 범위 보고서 패치 적용

AMS 패치 적용 SSM 적용 범위 보고서는 계정의 EC2 인스턴스에 SSM 에이전트가 설치되어 있는지 여부를 알려줍니다.

필드 이름	정의
고객 이름	하위 고객이 여러 명 있는 상황의 고객 이름
리소스 리전	AWS 리소스가 위치한 리전
계정 이름	계정의 이름입니다.
AWS 계정 ID	AWS 계정의 ID
Resource Id	EC2 인스턴스의 ID
Resource Name	EC2 인스턴스의 이름
규정 준수 플래그	리소스에 SSM 에이전트가 설치되어 있는지("규정 준수") 또는 설치되어 있지 않은지("NON_COMPLIANT") 나타냅니다.

AMS 백업 보고서

사용 가능한 보고서

- [백업 작업 성공/실패 보고서](#)
- [백업 요약 보고서](#)
- [백업 요약/보장 보고서](#)

백업 작업 성공/실패 보고서

백업 작업 성공/실패 보고서는 지난 몇 주 동안 실행된 백업에 대한 정보를 제공합니다. 보고서를 사용자 지정하려면 데이터를 검색할 주 수를 지정합니다. 기본 주 수는 12입니다. 다음 표에는 보고서에 포함된 데이터가 나열되어 있습니다.

필드 이름	정의
AWS 계정 ID	리소스가 속한 AWS 계정 ID
계정 이름	AWS 계정 이름
백업 작업 ID	백업 작업의 ID
리소스 ID	백업된 리소스의 ID
리소스 유형	백업 중인 리소스 유형
리소스 리전	백업된 리소스의 AWS 리전
백업 상태	백업의 상태입니다. 자세한 내용은 백업 작업 상태를 참조하세요 .
복구 시점 ID	복구 시점의 고유 식별자입니다.
상태 메시지	백업 작업 중에 발생한 오류 또는 경고에 대한 설명
백업 크기	GB 단위의 백업 크기
복구 시점 ARN	생성된 백업의 ARN
일 단위의 복구 시점 기간	복구 시점이 생성된 이후 경과한 일수
30일 미만	30일 미만의 백업 지표

백업 요약 보고서

필드 이름	정의
고객 이름	여러 하위 고객이 인 상황의 고객 이름
백업 월	백업 월
백업 연도	백업 연도
리소스 유형	백업 중인 리소스 유형
리소스 수	백업된 리소스 수
복구 시점 수	고유한 스냅샷 수
30일 미만의 백업	30일 미만의 백업 수
최대 복구 시점 수명	일 단위의 가장 오래된 복구 시점 수명
최소 복구 시점 수명	일 단위의 가장 최근 복구 시점 기간

백업 요약/보장 보고서

백업 요약/보장 보고서에는 현재 어떤 AWS Backup 계획으로도 보호되지 않는 리소스 수가 나열됩니다. 가능한 경우 적용 범위를 늘리고 데이터 손실 위험을 줄이기 위한 적절한 계획을 CDSM과 논의합니다.

필드 이름	정의
고객 이름	여러 하위 고객이 인 상황의 고객 이름
리전	AWS 리소스가 위치한 리전
계정 이름	계정의 이름입니다.
AWS 계정 ID	AWS 계정의 ID

필드 이름	정의
리소스 유형	리소스의 유형입니다. 리소스는 AWS Backup (Aurora, DocumentDB, DynamoDB, EBS, EC2, EFS, FSx, RDS 및 S3)에서 지원됩니다.
리소스 ARN	리소스의 ARN
리소스 ID	리소스의 ID
충당률	리소스가 포함되는지 여부를 나타냅니다("COVERED" 또는 "NOT_COVERED").
리소스 수	계정에서 지원되는 리소스 수
perc_coverage	지난 30일 동안 실행된 백업이 있는 지원되는 리소스의 백분율입니다.

인시던트 방지 및 상위 화자 보고서 모니터링

사용 가능한 보고서

- [인시던트 방지 보고서](#)
- [상위 화자 보고서 모니터링](#)

인시던트 방지 보고서

Incidents Prevented 보고서에는 자동으로 해결되어 발생할 수 있는 인시던트를 방지하는 Amazon CloudWatch 경보가 나열됩니다. 자세한 내용은 [자동 문제 해결](#)을 참조하세요. 다음 표에는 이 보고서에 포함된 정보가 나열되어 있습니다.

필드 이름	정의
실행_시작_시간_utc	자동화가 실행된 날짜
customer_name	계정 고객 이름
account_name	계정의 이름입니다.

필드 이름	정의
AwsAccountId	AWS 계정의 ID
document_name	실행된 SSM 문서 또는 자동화의 이름
duration_in_분	분 단위의 자동화 길이
리전	AWS 리소스가 위치한 리전
automation_execution_id	실행의 ID입니다.
automation_execution_status	실행 상태

상위 화자 보고서 모니터링

상위 화자 모니터링 보고서는 특정 기간 동안 생성된 Amazon CloudWatch 알림 수를 표시하고 가장 많은 수의 알림을 생성하는 리소스에 대한 시각화를 제공합니다. 이 보고서는 가장 많은 수의 알림을 생성하는 리소스를 식별하는 데 도움이 됩니다. 이러한 리소스는 근본 원인 분석을 수행하여 문제를 해결하거나 실제 문제가 없을 때 불필요한 트리거를 방지하기 위해 경보 임계값을 수정하는 데 적합할 수 있습니다. 다음 표에는 이 보고서에 포함된 정보가 나열되어 있습니다.

필드 이름	정의
고객 이름	고객 이름
AccountId	AWS 계정의 ID
알림 범주	트리거된 알림 유형
설명	알림에 대한 설명
리소스 ID	알림을 트리거한 리소스의 ID
Resource Name	알림을 트리거한 리소스의 이름
리전	AWS 리소스가 위치한 리전
인시던트 상태	경보에서 생성된 인시던트의 최신 상태

필드 이름	정의
첫 번째 발생	알림이 처음 트리거된 경우
최근 발생	알림이 트리거된 가장 최근 시간
알림 수	첫 번째 발생과 최근 발생 사이에 생성된 알림 수

결제 요금 세부 정보 보고서

AWS Managed Services(AMS) 결제 요금 세부 정보 보고서는 다음을 포함하여 연결된 계정 및 각 AWS 서비스의 AMS 결제 요금에 대한 세부 정보를 제공합니다.

- AMS 서비스 수준 요금, 증가 비율, 계정 수준 AMS 서비스 티어 및 AMS 요금.
- 연결된 계정 및 AWS 사용 요금

필드 이름	정의
결제 월	청구된 서비스의 월 및 연도
지급인 계정 ID	AMS 요금 지불을 담당하는 계정을 식별하는 12 자리 ID
연결된 계정 ID	비용을 생성하는 서비스를 사용하는 AMS 계정을 식별하는 12자리 ID
AWS 서비스 이름	사용된 AWS 서비스
AWS 요금	AWS 서비스 이름에 나열된 AWS 서비스 이름에 대한 AWS 요금
요금제	연결된 계정과 연결된 요금제의 이름입니다.
상승 비율	pricing_plan, SLA 및 AWS 서비스를 기반으로 한 상승 비율(10진수 V.WXYZ)
조정된 AWS 요금	AWS AMS에 맞게 조정된 사용량

필드 이름	정의
업리프팅된 AWS 요금	AMS에 대해 청구되는 AWS 요금의 비율입니다. $\text{adjusted\_aws\_charges} * \text{uplift\_percent}$
인스턴스 EC2 RDS 지출	EC2 및 RDS 인스턴스에 대한 지출
AMS 요금	제품에 대한 총 AMS 요금, $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$
비례 할당 최소 요금	계약 최소값을 충족하기 위해 청구되는 금액
최소 요금	AMS 최소 요금(해당하는 경우)
연결된 계정 총 AMS 요금	linked_account에 대한 모든 요금의 합계
지급인 계정 총 AMS 요금	지급인 계정에 대한 모든 요금의 합계

신뢰할 수 있는 수정자 보고서

사용 가능한 보고서

- [신뢰할 수 있는 수정자 수정 요약 보고서](#)
- [신뢰할 수 있는 수정자 구성 요약 보고서](#)
- [Trusted Advisor 요약 보고서 확인](#)

신뢰할 수 있는 수정자 수정 요약 보고서

신뢰할 수 있는 문제 해결자 문제 해결 상태 보고서는 이전 문제 해결 주기 동안 발생한 문제 해결에 대한 정보를 제공합니다. 기본 주 수는 1입니다. 보고서를 사용자 지정하려면 수정 일정에 따라 주 수를 지정합니다.

필드 이름	정의
날짜	데이터가 수집된 날짜입니다.
계정 ID	리소스가 속한 AWS 계정 ID

필드 이름	정의
계정 이름	AWS 계정 이름
범주 확인	AWS Trusted Advisor 검사 범주
이름 확인	수정 Trusted Advisor 검사의 이름입니다.
검사 ID	수정 Trusted Advisor 검사의 ID입니다.
실행 모드	특정 Trusted Advisor 검사에 대해 구성된 실행 모드
OpsItem ID	문제 해결을 Trusted Advisor 위해에서 생성한 OpsItem의 ID
OpsItem 상태	보고 Trusted Advisor 시에서 생성한 OpsItem의 상태
리소스 ID	문제 해결을 위해 생성된 리소스의 ARN

신뢰할 수 있는 수정자 구성 요약 보고서

신뢰할 수 있는 수정자 구성 요약 보고서는 각 Trusted Advisor 검사에 대한 현재 신뢰할 수 있는 수정자 수정자 구성에 대한 정보를 제공합니다.

필드 이름	정의
날짜	데이터가 수집된 날짜입니다.
계정 ID	구성이 적용되는 AWS 계정 ID입니다.
계정 이름	AWS 계정 이름
범주 확인	AWS Trusted Advisor 검사 범주
이름 확인	구성이 적용되는 수정 Trusted Advisor 검사의 이름입니다.

필드 이름	정의
검사 ID	구성이 적용되는 수정 Trusted Advisor 검사의 ID입니다.
실행 모드	특정 Trusted Advisor 검사에 대해 구성된 실행 모드
자동으로 재정의	구성된 경우 실행 모드를 자동화로 재정의하는 태그 패턴
수동 재정의	구성된 경우 실행 모드를 수동으로 재정의하는 태그 패턴

Trusted Advisor 요약 보고서 확인

Trusted Advisor 검사 요약 보고서는 현재 Trusted Advisor 검사에 대한 정보를 제공합니다. 이 보고서는 매주 문제 해결 일정 이후에 데이터를 수집합니다. 기본 주 수는 1입니다. 보고서를 사용자 지정하려면 문제 해결 주기에 따라 주 수를 지정합니다.

필드 이름	정의
날짜	데이터가 수집된 날짜입니다.
계정 ID	구성이 적용되는 AWS 계정 ID입니다.
고객 이름	AWS 계정 이름
범주 확인	AWS Trusted Advisor 검사 범주
이름 확인	구성이 적용되는 수정 Trusted Advisor 검사의 이름입니다.
검사 ID	구성이 적용되는 수정 Trusted Advisor 검사의 ID입니다.
상태	검사의 알림 상태입니다. 가능한 상태는 정상(녹색), 경고(노란색), 오류(빨간색) 또는 not_available입니다.

필드 이름	정의
플래그가 지정된 리소스	Trusted Advisor 검사에 의해 플래그가 지정된 (목록에 있는) AWS 리소스 수입니다.
무시된 리소스	가 숨김으로 표시 Trusted Advisor 하여 무시한 AWS 리소스 수입니다.
중요 상태의 리소스	중요 상태의 리소스 수
경고 상태의 리소스	경고 상태의 리소스 수

셀프 서비스 보고서

AWS Managed Services(AMS) 셀프 서비스 보고서(SSR)는 다양한 네이티브 AWS 서비스에서 데이터를 수집하고 주요 AMS 제품에 대한 보고서에 대한 액세스를 제공하는 기능입니다. SSR은 운영, 구성 관리, 자산 관리, 보안 관리 및 규정 준수를 지원하는 데 사용할 수 있는 정보를 제공합니다.

SSR을 사용하여 AMS 콘솔에서 보고서에 액세스하고 Amazon S3 버킷(계정당 버킷 1개)을 통해 데이터 세트를 보고합니다. 선호하는 비즈니스 인텔리전스(BI) 도구에 데이터를 연결하여 고유한 요구 사항에 따라 보고서를 사용자 지정할 수 있습니다. AMS는 기본 AWS 리전에서 S3 버킷(S3 버킷 이름: `ams-reporting-data-a<Account_ID>`)을 생성하고 us-east-1 리전에서 호스팅되는 AMS 컨트롤 플레인에서 데이터를 공유합니다.

Important

이 기능에 액세스하려면 다음 역할 중 하나가 있어야 합니다.

- 다중 계정 랜딩 존: `AWSSManagedServicesReadOnlyRole`
- 단일 계정 랜딩 존: `Customer_ReadOnly_Role`

Important

에서 사용자 지정 키 사용 AWS Glue

고객 관리형 KMS 키로 AWS Glue 메타데이터를 암호화하려면 AMS가 계정의 데이터를 집계할 수 있도록 다음 추가 단계를 수행해야 합니다.

1. <https://console.aws.amazon.com/kms> AWS Key Management Service 콘솔을 연 다음 고객 관리형 키를 선택합니다.
2. AWS Glue 메타데이터를 암호화하는 데 사용할 키 ID를 선택합니다.
3. 별칭 탭을 선택한 다음 별칭 생성을 선택합니다.
4. 텍스트 상자에 AmsReportingFlywheelCustomKey를 입력한 다음 별칭 생성을 선택합니다.

주제

- [내부 API 작업](#)
- [패치 보고서\(일별\)](#)
- [백업 보고서\(일별\)](#)
- [인시던트 보고서\(주별\)](#)
- [결제 보고서\(월별\)](#)
- [집계된 보고서](#)
- [AMS 셀프 서비스 보고서 대시보드](#)
- [데이터 보존 정책](#)
- [SSR에서 오프보드](#)

내부 API 작업

API 작업을 모니터링하는 경우 다음 내부 전용 작업에 대한 호출이 표시될 수 있습니다.

- GetDashboardUrl
- ListReportsV2

내부 API 작업: GetDashboardUrl

이 작업은 AMS 콘솔에서 호출할 때 시스템 로그에 표시됩니다. 다른 사용 사례는 없습니다. 직접 사용할 수 없습니다.

해당 보고서에 대한 임베디드 대시보드 URL을 반환합니다. 이 작업은에서 dashboardName 반환한를 수락합니다ListReports.

요청 구문

```
HTTP/1.1 200
Content-type: application/json
{
  "dashboardName": "string"
}
```

요청 요소

dashboardName: URL이 요청되는 QuickSight 대시보드의 이름입니다. 대시보드 이름은 ListReportsV2에 반환됩니다.

유형: 문자열

응답 구문

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반환합니다. 다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

url: 요청된에 대한 QuickSight URL을 반환합니다dashboardName.

유형: 문자열

오류

모든 작업에 공통적인 오류에 대한 자세한 내용은 [공통 오류를](#) 참조하세요.

BadRequestException:

제출된 요청이 유효하지 않습니다. 예를 들어 입력이 불완전하거나 잘못된 경우입니다. 자세한 내용은 함께 제공되는 오류 메시지를 참조하세요.

HTTP 상태 코드: 400

NotFoundException:

요청된 리소스를 찾을 수 없습니다. 요청 URI가 올바른지 확인합니다.

HTTP 상태 코드: 404

TooManyRequestsException:

요청이 제한 한도에 도달했습니다. 지정된 기간 후에 재시도합니다.

HTTP 상태 코드: 429

UnauthorizedException:

호출자의 권한이 충분하지 않아 요청이 거부됩니다.

HTTP 상태 코드: 401

내부 API 작업: ListReportsV2

이 API는 AMS 콘솔에서 호출할 때 시스템 로그에 나타납니다. 다른 사용 사례는 없습니다. 직접 사용할 수 없습니다.

지정된 계정에 사용할 수 있는 운영 보고서 목록을 반환합니다.

요청 구문

요청에 요청 본문이 없습니다.

응답 구문

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
      "dashboard": "string",
      "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반환합니다. 다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

reportsList: 사용 가능한 운영 보고서 목록입니다.

유형: 대시보드 객체 배열

reportsType: 보고서가 여러 계정에 걸쳐 집계되는지 여부를 나타냅니다.

유형: 문자열

오류

모든 작업에 공통적인 오류에 대한 자세한 내용은 [공통 오류를](#) 참조하세요.

BadRequestException:

제출된 요청이 유효하지 않습니다. 예를 들어 입력이 불완전하거나 올바르지 않습니다. 자세한 내용은 함께 제공되는 오류 메시지를 참조하세요.

HTTP 상태 코드: 400

NotFoundException:

요청된 리소스를 찾을 수 없습니다. 요청 URI가 올바른지 확인합니다.

HTTP 상태 코드: 404

TooManyRequestsException:

요청이 제한 한도에 도달했습니다. 지정된 기간 후에 재시도합니다.

HTTP 상태 코드: 429

UnauthorizedException:

호출자의 권한이 충분하지 않아 요청이 거부됩니다.

HTTP 상태 코드: 401

패치 보고서(일별)

사용 가능한 보고서

-
- [패치 세부 정보](#)

• 패치를 놓친 인스턴스

패치 오케스트레이터(PO)에 온보딩된 모든 인스턴스, 계정 상태, 인스턴스 세부 정보, 유지 관리 기간 적용 범위, 유지 관리 기간 실행 시간, 스택 세부 정보 및 플랫폼 유형을 식별하는 데 도움이 되는 정보 보고서입니다.

이 데이터 세트는 다음을 제공합니다.

- 계정의 프로덕션 및 비프로덕션 인스턴스에 대한 데이터입니다. 프로덕션 및 비프로덕션 단계는 인스턴스 태그가 아닌 계정 이름에서 파생됩니다.
- 플랫폼 유형별 인스턴스 배포에 대한 데이터입니다. 'N/A' 플랫폼 유형은 AWS Systems Manager(SSM)가 플랫폼 정보를 가져올 수 없을 때 발생합니다.
- 인스턴스 상태 분포, 실행, 중지 또는 종료 중인 인스턴스 수에 대한 데이터입니다.

콘솔 필드 이름	데이터 세트 필드 이름	정의
액세스 제한	access_restrictions	액세스가 제한된 리전
계정 ID	aws_account_id	AWS 인스턴스 ID가 속한 계정 ID
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
계정 이름	account_name	AWS 계정 이름
계정 상태	account_status	AMS 계정 상태
	account_sla	AMS 계정 서비스 약정
계정 유형	malz_role	MALZ 역할
오토 스케일링 그룹 이름	instance_asg_name	인스턴스가 포함된 Auto Scaling 그룹(ASG)의 이름
인스턴스 ID	instance-id	EC2 인스턴스의 ID

콘솔 필드 이름	데이터 세트 필드 이름	정의
인스턴스 이름	instance_name	EC2 인스턴스의 이름
인스턴스 패치 그룹	instance_patch_group	인스턴스를 그룹화하고 동일한 유지 관리 기간을 적용하는 데 사용되는 패치 그룹 이름
인스턴스 패치 그룹 유형	instance_patch_group_type	패치 그룹 유형
인스턴스 플랫폼 유형	instance_platform_type	운영 체제(OS) 유형
인스턴스 플랫폼 이름	instance_platform_name	운영 체제(OS) 이름
인스턴스 상태	instance_state	EC2 인스턴스 수명 주기 내의 상태
인스턴스 태그	ec2_tags	Amazon EC2 인스턴스 ID와 연결된 태그
랜딩 존	malz_flag	MALZ 관련 계정에 대한 플래그
유지 관리 기간 적용 범위	mw_covered_flag	인스턴스에 향후 실행 날짜가 있는 활성화된 유지 관리 기간이 하나 이상 있는 경우 해당 기간이 적용되는 것으로 간주되고 그렇지 않으면 적용되지 않습니다.
유지 관리 기간 실행 날짜/시간	earliest_window_execution_time	다음에 유지 관리 기간이 실행될 것으로 예상되는 경우
유지 관리 기간 실행 날짜/시간	earliest_window_execution_time	다음에 유지 관리 기간이 실행될 것으로 예상되는 경우

콘솔 필드 이름	데이터 세트 필드 이름	정의
프로덕션 계정	prod_계정	계정 이름에 'PROD', 'NONPROD' 값이 포함되는지 여부에 따라 AMS prod, 비prod 계정의 식별자입니다.
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜와 시간입니다.
[Stack Name]	인스턴스_스택_이름	인스턴스가 포함된 스택의 이름
스택 유형	인스턴스_스택_유형	AMS 스택(고객 계정 내 AMS 인프라) 또는 고객 스택(고객 애플리케이션을 지원하는 AMS 관리형 인프라)

패치 세부 정보

이 보고서는 다양한 인스턴스의 패치 세부 정보와 유지 관리 기간 범위를 제공합니다.

이 보고서는 다음을 제공합니다.

- 패치 그룹 및 해당 유형에 대한 데이터입니다.
- 유지 관리 기간, 기간, 마감, 향후 유지 관리 기간 실행 날짜(일정) 및 각 기간의 영향을 받는 인스턴스에 대한 데이터입니다.
- 계정의 모든 운영 체제에 대한 데이터와 운영 체제가 설치된 인스턴스 수입니다.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜와 시간입니다.
계정 ID	aws_account_id	AWS 인스턴스 ID가 속한 계정 ID

필드 이름	데이터 세트 필드 이름	정의
계정 이름	account_name	AWS 계정 이름
계정 상태	account_status	AMS 계정 상태
규정 준수 - 중요	compliant_critical	심각도가 "중요"인 규정 준수 패치 수
규정 준수 - 높음	compliant_high	심각도가 "높음"인 규정 준수 패치 수
규정 준수 - 중간	compliant_medium	심각도가 "중간"인 규정 준수 패치 수
규정 준수 - 낮음	compliant_low	심각도가 "낮음"인 규정 준수 패치 수
규정 준수 - 정보 제공	compliant_info	"정보" 심각도의 규정 준수 패치 수
규정 준수 - 지정되지 않음	compliant_unspecified	심각도가 "지정되지 않음"인 규정 준수 패치 수
규정 준수 - 합계	compliant_total	규정 준수 패치 수(모든 심각도)
인스턴스 ID	instance-id	EC2 인스턴스의 ID
인스턴스 이름	instance_name	EC2 인스턴스의 이름
	account_sla	AMS 계정 서비스 계층
인스턴스 플랫폼 유형	instance_platform_type	운영 체제(OS) 유형
인스턴스 플랫폼 이름	instance_platform_name	운영 체제(OS) 이름

필드 이름	데이터 세트 필드 이름	정의
인스턴스 패치 그룹 유형	instance_patch_group_type	DEFAULT: 인스턴스의 AMSDefaultPatchGroup:True 태그로 결정되는 기본 유지 관리 기간이 있는 기본 패치 그룹 고객: 고객이 생성한 패치 그룹 NOT_ASSIGNED: 패치 그룹이 할당되지 않음
인스턴스 패치 그룹	instance_patch_group	인스턴스를 그룹화하고 동일한 유지 관리 기간을 적용하는 데 사용되는 패치 그룹 이름
인스턴스 상태	instance_state	EC2 인스턴스 수명 주기 내의 상태
인스턴스 태그	ec2_tags	Amazon EC2 인스턴스 ID와 연결된 태그
마지막 실행 유지 관리 기간	last_execution_window	유지 관리 기간이 실행된 최근 시간
유지 관리 기간 ID	window_id	유지 관리 기간 ID
유지 관리 기간 상태	window_state	유지 관리 기간 상태
유지 관리 기간 유형	window_type	유지 관리 기간 유형
유지 관리 기간 다음 실행 날짜/시간	window_next execution_time	다음에 유지 관리 기간이 실행 될 것으로 예상되는 경우
유지 관리 기간(시간)	window_duration	유지 관리 기간의 지속 시간

필드 이름	데이터 세트 필드 이름	정의
유지 관리 기간 적용 범위	mw_covered_flag	인스턴스에 향후 실행 날짜가 있는 활성화된 유지 관리 기간이 하나 이상 있는 경우 해당 기간이 적용되는 것으로 간주되고 그렇지 않으면 적용되지 않습니다.
규정 미준수 - 중요	noncompliant_critical	심각도가 "중요"인 규정 미준수 패치 수
규정 미준수 - 높음	규정 미준수_높음	심각도가 "높음"인 규정 미준수 패치 수
규정 미준수 - 중간	규정 미준수_중간	심각도가 "중간"인 규정 미준수 패치 수
규정 미준수 - 낮음	규정 미준수_낮음	심각도가 "낮음"인 규정 미준수 패치 수
규정 미준수 - 정보 제공	규정 미준수_정보	심각도가 "정보"인 규정 미준수 패치 수
규정 미준수 - 지정되지 않음	규정 미준수_지정되지 않음	심각도가 "지정되지 않음"인 규정 미준수 패치 수
규정 미준수 - 합계	noncompliant_total	규정 미준수 패치 수(모든 심각도)
패치 기준 ID	patch_Baseline_id	현재 인스턴스에 연결된 패치 기준

필드 이름	데이터 세트 필드 이름	정의
패치 상태	patch_status	전체 패치 규정 준수 상태입니다. 누락된 패치가 하나 이상 있는 경우 인스턴스는 규정을 준수하지 않는 것으로 간주되고, 그렇지 않으면 규정을 준수하는 것으로 간주됩니다.
프로덕션 계정	prod_계정	계정 이름에 'PROD', 'NONPROD' 값이 포함되는지 여부에 따라 AMS prod, 비prod 계정의 식별자입니다.
스택 유형	인스턴스_스택_유형	AMS 스택(고객 계정 내 AMS 인프라) 또는 고객 스택(고객 애플리케이션을 지원하는 AMS 관리형 인프라)
	window_next_exec_yyyy	window_next_execution_time의 연도 부분
	window_next_exec_mm	window_next_execution_time의 월 부분
	window_next_exec_D	window_next_execution_time의 요일 부분
	window_next_exec_HHMM	window_next_execution_time의 시간:분 부분

패치를 놓친 인스턴스

이 보고서는 마지막 유지 관리 기간 실행 중에 패치를 놓친 인스턴스에 대한 세부 정보를 제공합니다.

이 보고서는 다음을 제공합니다.

- 패치 ID 수준에서 누락된 패치에 대한 데이터입니다.

- 패치가 하나 이상 누락된 모든 인스턴스의 데이터 및 패치 심각도, 패치가 적용되지 않은 날짜, 범위 및 패치 릴리스 날짜와 같은 속성.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간
계정 ID	aws_account_id	AWS 인스턴스 ID가 속한 계정 ID
계정 이름	account_name	AWS 계정 이름
고객 이름 상위	customer_name_parent	
고객 이름	customer_name	
프로덕션 계정	prod_계정	계정 이름에 'PROD' 또는 'NONPROD' 값이 포함되는지 여부에 따라 AMS prod 또는 비 prod 계정의 식별자입니다.
계정 상태	account_status	AMS 계정 상태
계정 유형	account_type	
	account_sla	AMS 계정 서비스 티어
인스턴스 ID	instance-id	EC2 인스턴스의 ID
인스턴스 이름	instance_name	EC2 인스턴스의 이름
인스턴스 플랫폼 유형	instance_platform_type	운영 체제(OS) 유형
인스턴스 상태	instance_state	EC2 인스턴스 수명 주기 내의 상태
인스턴스 태그	ec2_tags	Amazon EC2 인스턴스 ID와 연결된 태그
패치 ID	patch_id	릴리스된 패치의 ID

필드 이름	데이터 세트 필드 이름	정의
패치 심각도	patch_sev	게시자당 패치 심각도
패치 분류	patch_class	패치 게시자당 패치 분류
패치 릴리스 날짜/시간(UTC)	release_dt_utc	게시자당 패치 릴리스 날짜
패치 설치 상태	install_state	SSM당 인스턴스에 패치 상태 설치
패치되지 않은 일수	days_unpatched	마지막 SSM 스캔 이후 인스턴스가 패치되지 않은 일수
패치되지 않은 일수 범위	days_unpatched_bucket	패치되지 않은 일수의 버킷팅

백업 보고서(일별)

백업 보고서는 기본 및 보조(해당하는 경우) 리전을 다룹니다. 백업 상태(성공/실패)와 생성된 스냅샷에 대한 데이터를 다룹니다.

이 보고서는 다음을 제공합니다.

- 백업 상태
- 생성된 스냅샷 수
- 복구 시점
- 백업 계획 및 볼트 정보

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜와 시간입니다.
계정 ID	aws_account_id	인스턴스 ID가 속한 AWS 계정 ID

필드 이름	데이터 세트 필드 이름	정의
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
계정 이름	account_name	AWS 계정 이름
계정 SLA	account_sla	AMS 계정 서비스 약정
	malz_flag	MALZ 관련 계정에 대한 플래그
	malz_role	MALZ 역할
	access_restrictions	액세스가 제한된 리전
백업 스냅샷 예약 시작 날짜/시간	시작_바이_dt_utc	스냅샷이 시작되도록 예약된 시점의 타임스탬프
백업 스냅샷 실제 시작 날짜/시간	생성_dt_utc	스냅샷이 실제로 시작될 때의 타임스탬프
백업 스냅샷 완료 날짜/시간	completion_dt_utc	스냅샷 완료 시 타임스탬프
백업 스냅샷 만료 날짜/시간	expiration_dt_utc	스냅샷 만료 시 타임스탬프
백업 작업 상태	backup_job_status	스냅샷의 상태
백업 유형	backup_type	백업 유형
백업 작업 ID	backup_job_id	백업 작업의 고유 식별자
바이트 단위의 백업 크기	backup_size_in_바이트	바이트 단위의 백업 크기
백업 계획 ARN	backup_plan_arn	백업 계획 ARN
백업 계획 ID	backup_plan_id	백업 계획 고유 식별자
백업 계획 이름	backup_plan_이름	백업 계획 이름

필드 이름	데이터 세트 필드 이름	정의
백업 계획 버전	backup_plan_버전	백업 계획 버전
백업 규칙 ID	backup_rule_id	백업 규칙 ID
백업 볼트 ARN	backup_vault_arn	백업 볼트 ARN
백업 볼트 이름	backup_vault_이름	백업 볼트 이름
IAM 역할 ARN	iam_role_arn	IAM 역할 ARN
인스턴스 ID	instance-id	고유 인스턴스 ID
인스턴스 상태	instance_state	인스턴스 상태
인스턴스 태그	ec2_tags	EC2 인스턴스 ID와 연결된 태그
리소스 ARN	resource_arn	Amazon 리소스 이름
Resource Id	resource_id	고유한 리소스 식별자
리소스 리전	resource_region	리소스의 기본(및 해당하는 경우 보조) 리전입니다.
리소스 유형	resource_type	리소스 유형
복구 시점 ARN	recovery_point_arn	복구 시점의 ARN
복구 시점 ID	recovery_point_id	복구 시점의 고유 식별자입니다.
복구 시점 상태	recovery_point_status	복구 시점 상태
일 후 복구 시점 삭제	recovery_point_delete_after_days	일 후 복구 시점 삭제
며칠 후 콜드 스토리지로 복구 시점 이동	recovery_point_move_to_cold_storage_after_days	백업 스냅샷이 콜드 스토리지로 이동된 완료 날짜 이후 일수

필드 이름	데이터 세트 필드 이름	정의
복구 시점 암호화 상태	recovery_point_is_encrypted	복구 시점 암호화 상태
복구 시점 암호화 키 ARN	recovery_point_encryption_key_arn	복구 시점 암호화 키 ARN
스택 ID	stack_id	Cloudformation 스택 고유 식별자
[Stack Name]	stack_name	[Stack Name]
태그: AMS 기본 패치 그룹	tag_ams_default_patch_group	태그 값: AMS 기본 패치 그룹
태그: 앱 ID	tag_app_id	태그 값: 앱 ID
태그: 앱 이름	tag_app_name	태그 값: 앱 이름
태그: 백업	tag_backup	태그 값: 백업
태그: 규정 준수 프레임워크	tag_compliance_framework	태그 값: 규정 준수 프레임워크
태그: 비용 센터	tag_cost_center	태그 값: 비용 센터
태그: 고객	태그_고객	태그 값: 고객
태그: 데이터 분류	tag_data_classification	태그 값: 데이터 분류
태그: 환경 유형	tag_environment_type	태그 값: 환경 유형
태그: 운영 시간	작업_시간_태그	태그 값: 운영 시간
태그: 소유자 팀	tag_owner_team	태그 값: 소유자 팀
태그: 소유자 팀 이메일	tag_owner_team_email	태그 값: 소유자 팀 이메일
태그: 패치 그룹	tag_patch_group	태그 값: 패치 그룹
태그: 지원 우선 순위	tag_support_priority	태그 값: 지원 우선 순위
볼륨 상태	volume_state	볼륨 상태

인시던트 보고서(주별)

이 보고서는 다음을 포함하여 우선순위, 심각도 및 최신 상태와 함께 집계된 인시던트 목록을 제공합니다.

- 관리형 계정에서 인시던트로 분류된 지원 사례에 대한 데이터
- 관리형 계정의 인시던트 지표를 시각화하는 데 필요한 인시던트 정보
- 모든 인시던트의 인시던트 범주 및 문제 해결 상태에 대한 데이터

주간 인시던트 보고서에는 시각화와 데이터를 모두 사용할 수 있습니다.

- 시각화는 보고서 페이지를 통해 계정의 AMS 콘솔을 통해 액세스할 수 있습니다.
- 다음 스키마가 있는 데이터 세트는 관리형 계정의 S3 버킷을 통해 액세스할 수 있습니다.
- 제공된 날짜 필드를 사용하여 인시던트가 생성되거나 해결된 월, 분기, 주 및/또는 날짜를 기준으로 인시던트를 필터링합니다.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간입니다.
계정 ID	aws_account_id	AWS 인시던트가 속한 계정 ID입니다.
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
계정 이름	account_name	AWS 계정 이름입니다.
사례 ID	case_id	인시던트의 ID입니다.
생성된 월	생성_월	인시던트가 생성된 달입니다.
우선순위	priority	인시던트의 우선 순위입니다.
심각도	severity	인시던트의 심각도입니다.

필드 이름	데이터 세트 필드 이름	정의
상태	status	인시던트의 상태입니다.
범주	yuma_category	인시던트의 범주입니다.
생성된 날짜	생성_일	인시던트가 YYYY-MM-DD 형식으로 생성된 날짜입니다.
생성된 주	created_wk	인시던트가 YYYY-WW 형식으로 생성된 주입니다. 일요일부터 토요일까지는 일주일의 시작과 끝으로 계산됩니다. 주 단위는 01~52입니다. 01주차는 항상 연도의 첫날이 포함된 주입니다. 예를 들어 2023-12-31 및 2024-01-01은 2024년 1월에 있습니다.
생성된 분기	created_qtr	인시던트가 YYYY-Q 형식으로 생성된 분기입니다. 01/01~03/31은 Q1 등으로 정의됩니다.
해결된 날짜	resolved_day	인시던트가 YYYY-MM-DD 형식으로 해결된 날짜입니다.
해결된 주	Resolve_wk	인시던트가 YYYY-WW 형식으로 해결된 주입니다. 일요일부터 토요일까지는 일주일의 시작과 끝으로 계산됩니다. 주 단위는 01~52입니다. 01주차는 항상 연도의 첫날이 포함된 주입니다. 예를 들어, 2023-12-31 및 2024-01-01은 2024년 1주차입니다.
해결된 월	resolved_month	인시던트가 YYYY-MM 형식으로 해결된 달입니다.

필드 이름	데이터 세트 필드 이름	정의
해결된 분기	해석됨_qtr	인시던트가 YYYY-Q 형식으로 해결된 분기입니다. 01/01~03/31은 Q1 등으로 정의됩니다.
생성된 그룹화 규칙	그룹화_규칙	인시던트에 적용되는 그룹화 규칙입니다. "no_grouping" 또는 "instance_grouping".
인스턴스 ID	instance_ids	인시던트와 연결된 인스턴스입니다.
알림 수	number_of_alerts	해당 인시던트와 연결된 알림 수입니다. 그룹화를 활성화한 경우 이 숫자는 1보다 클 수 있습니다. 그룹화를 활성화하지 않은 경우 항상 1이 됩니다.
생성 시간	created_at	인시던트가 생성된 시점의 타임스탬프입니다.
경보 ARNs	alarm_arns	인시던트와 관련된 경보의 Amazon 리소스 이름("arn")입니다.
관련 경보	related_alarms	인시던트와 관련된 모든 경보의 사람이 읽을 수 있는 이름입니다.

결제 보고서(월별)

결제 요금 세부 정보

이 보고서는 연결된 계정 및 각 AWS 서비스의 AMS 청구 요금에 대한 세부 정보를 제공합니다.

이 보고서는 다음을 제공합니다.

- AMS 서비스 수준 요금, 증가율, 계정 수준 AMS 서비스 티어 및 AMS 요금에 대한 데이터입니다.

- 연결된 계정 및 AWS 사용 요금에 대한 데이터입니다.

 Important

월별 결제 보고서는 Management Payer Account(MPA) 또는 정의된 요금 계정에서만 사용할 수 있습니다. AMS 월별 청구서가 전송되는 계정입니다. 이러한 계정을 찾을 수 없는 경우 Cloud Service Delivery Manager(CSDM)에 문의하여 지원을 받으세요.

필드 이름	데이터 세트 필드 이름	정의
결제 날짜	date	청구된 서비스의 월 및 연도
지급인 계정 ID	payer_account_id	AMS 요금 지불을 담당하는 계정을 식별하는 12자리 ID
연결된 계정 ID	linked_account_id	확장을 생성하는 서비스를 사용하는 AMS 계정을 식별하는 12자리 ID
AWS 서비스 이름	product_name	사용된 AWS 서비스
AWS 요금	aws_charges	AWS 서비스 이름의 AWS 서비스 이름에 대한 AWS 요금
요금제	요금제	연결된 계정과 연결된 요금제
AMS 서비스 그룹	tier_uplifting_groups	상승 비율을 결정하는 AMS 서비스 그룹 코드
상승 비율	uplift_percent	pricing_plan, SLA 및 AWS 서비스를 기반으로 한 상승 비율 (10진수 V.WXYZ)
조정된 AWS 요금	adjusted_aws_usage	AWS AMS에 대해 조정된 사용량

필드 이름	데이터 세트 필드 이름	정의
업리프트된 AWS 요금	uplifted_aws_charges	AMS에 대해 청구되는 AWS 요금의 비율입니다. $\text{adjusted\_aws\_charges} * \text{uplift\_percent}$
인스턴스 EC2 RDS 지출	인스턴스_ec2_rds_spend	EC2 및 RDS 인스턴스에 대한 지출
예약 인스턴스 요금	ris_charges	예약 인스턴스 요금
업그레이드된 예약 인스턴스 요금	uplifted_ris	AMS에 대해 청구할 예약 인스턴스 요금의 백분율입니다. $\text{ris\_charges} * \text{uplift\_percent}$
Savings Plan 요금	sp_charges	SavingsPlan 사용 요금
업리프팅된 Savings Plan 요금	uplifted_sp	AMS에 대해 청구되는 절감형 플랜 요금의 비율, $\text{sp\_charges} * \text{uplift\_percent}$
AMS 요금	ams_charges	제품에 대한 총 ams 요금, $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$
비례 할당 최소 요금	비례 할당_최소	계약 최소값을 충족하기 위해 청구하는 금액
연결된 계정 총 AMS 요금	linked_account_total ams_charges	linked_account에 대한 모든 요금의 합계
지급인 계정 총 AMS 요금	payer_account_total ams_charges	지급인 계정에 대한 모든 요금의 합계
최소 요금	minimum_fees	AMS 최소 요금(해당하는 경우)

필드 이름	데이터 세트 필드 이름	정의
예약 인스턴스 및 Savings Plan 할인	adj_ri_sp_charges	RI/SP 요금에 적용되는 RI/SP 할인(특정 상황에서 적용)

집계된 보고서

집계된 셀프 서비스 보고(SSR)를 사용하면 조직 수준, 교차 계정에서 집계된 기존 셀프 서비스 보고서를 볼 수 있습니다. 이를 통해 내 AMS 관리 중인 모든 계정에서 패치 규정 준수, 백업 적용 범위 및 인시던트와 같은 주요 운영 지표를 파악할 수 있습니다 AWS Organizations.

집계된 SSR은 AWS Managed Services를 사용할 수 AWS 리전 있는 모든 상용에서 사용할 수 있습니다. 사용 가능한 리전의 전체 목록은 [리전 표](#)를 참조하세요.

집계된 보고서 활성화

AWS Organizations [관리 계정](#)에서 집계된 SSR을 관리해야 합니다. 관리 계정은 조직을 생성하는 데 사용한 AWS 계정입니다.

AMS에 온보딩된 AWS Organizations 관리 계정에 대해 집계된 SSR을 활성화하려면 AMS 콘솔에 액세스하고 보고서로 이동합니다. top-right-hand 모서리에서 조직 액세스를 선택하여 [AWS Managed Services 콘솔: 조직 보기](#) 창을 엽니다. 이 창에서 집계된 SSR 기능을 관리할 수 있습니다.

AWS Organizations AMS에 온보딩되지 않은 관리 계정은 AMS 콘솔에 액세스할 수 없습니다. AMS에 온보딩되지 않은 AWS Organizations 관리 계정에 대해 집계된 SSR을 활성화하려면 먼저 인증한 AWS 계정다음 [AWS 콘솔](#)로 이동하여 관리형 서비스를 검색합니다. 그러면 AMS Marketing 페이지가 열립니다. 이 페이지에서 탐색 모음의 조직 액세스 링크를 선택하여 집계된 SSR 기능을 관리할 수 있는 AWS Managed Services 콘솔: 조직 보기를 엽니다.

[AWS Managed Services 콘솔: Organization View](#)에 처음 액세스할 때 다음 단계를 완료합니다.

1. 아직 설정하지 않은 경우 콘솔에서 활성화 AWS Organizations를 AWS Organizations선택합니다. 설정에 대한 자세한 내용은 [AWS Organizations 사용 설명서](#)를 AWS Organizations참조하세요. 이 미를 사용하고 있는 경우이 단계를 건너뛸 수 있습니다 AWS Organizations.
2. 집계된 셀프 서비스 보고 서비스를 활성화하려면 콘솔에서 신뢰할 수 있는 액세스 활성화를 선택합니다.
3. (선택 사항) 조직 보기에 대한 읽기 액세스 권한을 갖도록 위임된 관리자를 등록합니다.

위임된 관리자로 집계된 보고서 보기

위임된 관리자는 집계된 보고서에 대한 읽기 액세스 권한을 갖도록 선택한 계정입니다. 위임된 관리자는 AMS에 온보딩된 계정이어야 하며 집계된 보고서에 대한 읽기 액세스 권한이 있는 유일한 계정이어야 합니다.

위임된 관리자를 선택하려면 AWS Managed Services 콘솔: 조직 보기의 3단계에 계정 ID를 입력합니다. 한 번에 하나의 위임된 관리자 계정만 등록할 수 있습니다. 위임된 관리자 계정은 AMS 관리 계정이어야 합니다.

위임된 관리자 계정을 업데이트하려면 [AWS Managed Services 콘솔: 조직 보기](#)로 이동하여 위임된 관리자 제거를 선택합니다. 콘솔에 위임된 관리자로 등록할 새 계정 ID를 삽입하라는 메시지가 표시됩니다.

집계된 보고서 읽기

위임된 관리자를 등록하지 않고 AWS Organizations 관리 계정이 AMS에 온보딩된 경우 AWS Organizations 관리 계정은 기본적으로 집계된 보고서에 대한 읽기 액세스 권한을 갖게 됩니다. AWS Organizations 관리 계정이 AMS에서 관리되지 않는 경우 집계된 보고서에 대한 읽기 액세스 권한을 가질 위임된 관리자 계정을 선택해야 합니다.

언제든지 AMS에 온보딩된 단일 계정만 AWS Organizations 관리 계정 또는 등록된 위임된 관리자인 집계된 보고서에 대한 읽기 액세스 권한을 가집니다. 조직 내(및 AMS에 온보딩된) 다른 모든 멤버 계정은 여전히 각 개별 계정의 단일 계정 보고서에만 액세스할 수 있습니다.

집계된 SSR을 활성화한 후 [보고서](#)로 이동합니다. 모든 기존 셀프 서비스 보고서가 이 섹션에 나열되고 파란색 태그는 보고서가 집계되었음을 나타냅니다. 집계된 보고서에 대한 읽기 액세스 권한을 갖도록 선택한 계정에서 AMS 콘솔에 액세스해야 합니다. 관리 AWS Organizations 계정 또는 위임된 관리자 계정입니다.

집계된 SSR을 활성화하면 다음 보고 주기부터 집계된 보고서를 사용할 수 있습니다.

집계된 보고서 비활성화

집계된 SSR을 비활성화하려면 [AWS Managed Services 콘솔: 조직 보기](#)를 엽니다. 신뢰할 수 있는 액세스 비활성화를 선택합니다. 집계된 SSR에 대해 신뢰할 수 있는 액세스를 비활성화하면 AMS 셀프 서비스 보고서가 조직 수준에서 계정 간에 집계되지 않습니다. 또한 비활성화는 다음 보고 주기부터 적용됩니다.

집계된 SSR을 비활성화한 후 AMS 콘솔의 보고서가 단일 계정 보고서로 나타나기까지 대기합니다. 이 지연은 다음 보고 주기부터 기능 비활성화가 적용되기 때문에 발생합니다.

AMS 셀프 서비스 보고서 대시보드

AMS 셀프 서비스 보고서는 [Resource Tagger 대시보드](#) 및의 두 가지 대시보드를 제공합니다. [보안 구성 규칙 대시보드](#).

Resource Tagger 대시보드

AMS 리소스 태거 대시보드는 Resource Tagger에서 지원하는 리소스에 대한 자세한 정보와 Resource Tagger가 해당 리소스에 적용하도록 구성된 태그의 현재 상태를 제공합니다.

리소스 유형별 리소스 태거 적용 범위

이 데이터 세트는 Resource Tagger에서 관리하는 태그가 있는 리소스 목록으로 구성됩니다.

리소스 유형별 리소스 적용 범위는 다음 지표를 설명하는 네 개의 선 차트로 시각화됩니다.

- 리소스 수: 리소스 유형별 리전의 총 리소스 수입니다.
- 관리형 태그가 누락된 리소스: 관리형 태그가 필요하지만 Resource Tagger에 의해 태그가 지정되지 않은 리소스 유형별 리전의 총 리소스 수입니다.
- 비관리형 리소스: Resource Tagger에서 관리형 태그를 적용하지 않은 리전의 리소스 유형별 총 수입니다. 이는 일반적으로 이러한 리소스가 Resource Tagger 구성과 일치하지 않거나 구성에서 명시적으로 제외됨을 의미합니다.
- 관리형 리소스: 비관리형 리소스 지표(리소스 수 - 비관리형 리소스)와 상응합니다.

다음 표에는이 보고서에서 제공하는 데이터가 나열되어 있습니다.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간 (UTC 시간)
AWS 계정 ID	aws_account_id	AWS 계정 ID
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
리전	리전	AWS 리전

필드 이름	데이터 세트 필드 이름	정의
리소스 유형	resource_type	이 필드는 리소스 유형을 식별합니다. Resource Tagger에서 지원하는 리소스 유형만 포함됩니다.
리소스 수	resource_count	이 리전에 배포된 리소스 수(지정된 리소스 유형)입니다.
ResourcesMissingManagedTags	resource_missing_managed_tags_count	구성 프로필에 따라 관리형 태그가 필요하지만 아직 Resource Tagger에서 태그를 지정하지 않은 리소스 수(지정된 리소스 유형)입니다.
UnmanagedResources	unmanaged_resource_count	Resource Tagger에서 관리형 태그를 적용하지 않은 리소스 수(지정된 리소스 유형)입니다. 일반적으로 이러한 리소스는 Resource Tagger 구성 블록과 일치하지 않거나 구성 블록에서 명시적으로 제외됩니다.

Resource Tagger 구성 규칙 규정 준수

이 데이터 세트는 리소스 유형 AWS 리전별로 특정 구성 프로필이 적용된 리소스 목록으로 구성됩니다. 선 차트로 시각화됩니다.

다음 표에는 이 보고서에서 제공하는 데이터가 나열되어 있습니다.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간(UTC 시간)
AWS 계정 ID	aws_account_id	AWS 계정 ID

필드 이름	데이터 세트 필드 이름	정의
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
리전	리전	AWS 리전
리소스 유형	resource_type	이 필드는 리소스 유형을 식별합니다. Resource Tagger에서 지원하는 리소스 유형만 포함됩니다.
구성 프로파일 ID	configuration_profile_id	Resource Tagger 구성 프로파일의 ID입니다. 구성 프로파일은 리소스에 태그를 지정하는 데 사용되는 정책 및 규칙을 정의하는 데 사용됩니다.
MatchingResourceCount	resource_count	Resource Tagger 구성 프로파일 ID와 일치하는 리소스 수(지정된 리소스 유형)입니다. 리소스가 구성 프로파일과 일치하려면 프로파일을 활성화하고 리소스가 프로파일의 규칙과 일치해야 합니다.

Resource Tagger 규정 미준수 리소스

이 데이터 세트는 단일 Resource Tagger 구성에 대해 규정을 준수하지 않는 리소스 목록으로 구성됩니다. 이 데이터는 리소스 규정 준수의 일일 스냅샷으로, 이러한 보고서가 고객 계정에 전달되는 시점의 고객 리소스 상태를 보여줍니다(기록 보기는 없음). 지정된 구성에 대해 불만이 없는 리소스로 구성된 피벗 테이블로 시각화됩니다.

다음 표에는 이 보고서에서 제공하는 데이터가 나열되어 있습니다.

필드 이름	데이터 세트 필드 이름	정의
보고서 날짜/시간	dataset_datetime	보고서가 생성된 날짜 및 시간 (UTC 시간)
AWS 계정 ID	aws_account_id	AWS 계정 ID
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
리전	리전	AWS 리전
리소스 유형	resource_type	이 필드는 리소스 유형을 식별합니다. Resource Tagger에서 지원하는 리소스 유형만 포함됩니다.
리소스 ID	resource_id	Resource Tagger에서 지원하는 리소스의 고유 식별자입니다.
적용 범위 상태	coverage_state	이 필드는 리소스가 Resource Tagger 구성 ID에 의해 구성된 대로 태그가 지정되었는지 여부를 나타냅니다.
구성 프로필 ID	configuration_profile_id	Resource Tagger 구성 프로필의 ID입니다. 구성 프로파일은 리소스에 태그를 지정하는 데 사용되는 정책 및 규칙을 정의하는 데 사용됩니다.

보안 구성 규칙 대시보드

보안 구성 규칙 대시보드는 AMS 계정의 리소스 및 AWS Config 규칙 규정 준수를 자세히 살펴봅니다. 보고서를 규칙 심각도별로 필터링하여 가장 중요한 조사 결과의 우선순위를 지정할 수 있습니다. 다음 표에는 이 보고서에서 제공하는 데이터가 나열되어 있습니다.

필드 이름	데이터 세트 필드 이름	정의
AWS 계정 ID	AWS 계정 ID	관련 리소스에 연결된 계정 ID입니다.
관리자 계정 ID	aws_admin_account_id	신뢰할 수 있는 AWS Organizations 계정이 활성화되어 있습니다.
보고서 날짜/시간	보고서 날짜	보고서가 생성된 날짜와 시간입니다.
customer_name	고객 이름	고객 이름입니다.
account_name	계정 이름	계정 ID와 연결된 이름
resource_id	리소스 ID	리소스의 식별자입니다.
resource_region	리소스 리전	리소스가 AWS 리전 있는 입니다.
resource_type	리소스 유형	AWS 서비스 또는 리소스 유형입니다.
resource_name	Resource Name	리소스의 이름입니다.
resource_ams_flag	리소스 AMS 플래그	리소스가 AMS 소유인 경우이 플래그는 TRUE로 설정됩니다. 리소스가 고객 소유인 경우이 플래그는 FALSE로 설정됩니다. 소유권을 알 수 없는 경우이 플래그는 UNKNOWN으로 설정됩니다.
config_rule	Config 규칙	구성 규칙의 사용자 지정할 수 없는 이름입니다.
config_rule_description	구성 규칙 설명	구성 규칙에 대한 설명입니다.

필드 이름	데이터 세트 필드 이름	정의
source_identifier	소스 식별자	관리형 구성 규칙의 고유 식별자이며 사용자 지정 구성 규칙의 식별자는 없습니다.
규정 준수_플래그	규정 준수 플래그	리소스가 구성 규칙을 준수하는지 또는 준수하지 않는지를 표시합니다.
rule_type	규칙 유형	규칙이 사전 정의인지 사용자 지정 빌드인지 나타냅니다.
exception_flag	예외 플래그	리소스 예외 플래그는 규정 미준수 리소스에 대한 위험 수락을 보여줍니다. 리소스에 대한 리소스 예외 플래그가 TRUE인 경우 리소스는 제외됩니다. 예외 플래그가 NULL인 경우 리소스는 제외되지 않습니다.
cal_dt	날짜	규칙의 평가 날짜입니다.
remediation_description	문제 해결 설명	규칙 규정 준수를 해결하는 방법에 대한 설명입니다.
severity	심각도	구성 규칙 심각도는 규정 미준수의 영향을 나타냅니다.
customer_action	고객 작업	따라서 규칙을 수정하는 데 필요한 작업입니다.
권장 사항	권장 사항	구성 규칙이 확인하는 항목에 대한 설명입니다.
문제 해결_범주	문제 해결 범주	이 규칙을 준수하지 않을 때 AMS가 수행하는 기본 작업입니다.

데이터 보존 정책

AMS SSR에는 보고된 기간, 데이터가 지워지고 더 이상 사용할 수 없게 된 후 보고서당 데이터 보존 정책이 있습니다.

보고서 이름	데이터 보존 SSR 콘솔	데이터 보존 SSR S3 버킷
인스턴스 세부 정보 요약(패치 오케스트레이터)	2개월	2년
패치 세부 정보	2개월	2년
유지 관리 기간 실행 중에 패치를 놓친 인스턴스	2개월	2년
AMS 결제 요금 세부 정보	2년	2년
일별 백업 보고서	1개월	2년
주간 인시던트 보고서	2개월	2년
보안 구성 규칙 대시보드	3개월	2년
Resource Tagger 대시보드	1년	2년

SSR에서 오프보드

SSR 서비스에서 오프보드하려면 AMS 콘솔을 통해 서비스 요청(SR)을 생성합니다. SR을 제출하면 AMS 운영 엔지니어가 SSR에서 오프보딩하는 데 도움을 줍니다. SR에서 오프보딩하려는 이유를 입력합니다.

계정을 오프보딩하고 리소스 정리를 수행하려면 AMS 콘솔을 통해 SR을 생성합니다. SR을 제출하면 AMS 운영 엔지니어가 SSR Amazon S3 버킷을 삭제하는 데 도움을 줍니다.

AMS에서 오프보딩하면 AMS SSR 콘솔에서 자동으로 오프보딩됩니다. AMS는 자동으로 사용자 계정으로 데이터 전송을 중지합니다. AMS는 오프보딩 프로세스의 일부로 SSR S3 버킷을 삭제합니다.

AMS의 인시던트 보고서, 서비스 요청 및 결제 질문

주제

- [인시던트 관리](#)
- [서비스 요청 관리](#)
- [결제 질문](#)

AWS Managed Services(AMS)를 사용하면 AMS 콘솔을 통해 언제든지 운영 문제 및 요청에 대한 지원을 요청할 수 있습니다. AMS 운영 엔지니어는 선택한 계정 서비스 티어(Plus, Premium)에 따라 응답 시간 서비스 수준 계약(SLAs) 및 서비스 수준 목표(SLOs)를 사용하여 인시던트 및 서비스 요청에 연중 무휴로 응답할 수 있습니다. AMS 운영 엔지니어는 동일한 메커니즘을 사용하여 중요한 알림 및 질문을 사전에 알립니다.

인시던트 관리

주제

- [인시던트 관리란 무엇입니까?](#)
- [인시던트 관리 서비스 약정](#)
- [인시던트 관리 예제](#)

인시던트는 AWS Managed Services(AMS) 또는 사용자의 결정에 따라 관리형 환경에 영향을 미치는 AWS 서비스 성능 문제입니다. AMS 팀이 식별한 인시던트는 먼저 모니터링으로 캡처된 시스템 상태의 변경인 "이벤트"로 수신됩니다. 구성된 임계값이 위반되면 이벤트는 알림이라고도 하는 경보를 트리거합니다. AMS 운영 팀은 이벤트가 영향을 미치지 않는지, 인시던트(서비스 중단 또는 성능 저하) 또는 문제(하나 이상의 해결된 인시던트의 근본 원인)인지 확인합니다.

또한 AMS 팀은 서비스 코드와 함께 [AWS Support API](#)를 사용하여 지원 센터 또는 프로그래밍 방식으로 식별한 인시던트를 수신합니다sentinel-report-incident.

AMS 운영 팀에서 인시던트를 수신한 후에는 인시던트가 서비스 요청으로 더 잘 분류되지 않도록 검토됩니다. 서비스 요청으로 분류해야 하는 경우 즉시 재분류되고 AMS 서비스 요청 팀이 인계하여 사용자에게 알립니다. 수신 운영자가 인시던트를 해결할 수 있는 경우 인시던트를 해결하기 위한 조치를 즉시 취합니다. AMS 운영자는 해결 방법은 내부 설명서를 참조하고 필요한 경우 인시던트가 해결될 때까지 다른 지원 리소스로 인시던트를 에스컬레이션합니다. 인시던트 해결 프로세스의 각 단계에서 정보를 받으려면 CC 이메일 옵션을 작성해야 하며, 페더레이션으로 연결하는 경우 AMS가 보내는 이메일

일의 링크를 따르기 전에 로그인해야 합니다. 해결되면 AMS 운영 팀은 나중에 사용할 수 있도록 인시던트와 해결 방법을 문서화합니다.

인시던트 해결에 인프라 변경이 필요한 경우 보안 검토가 필요할 수 있습니다. 보안 검토가 필요할 수 있는 인프라 변경에는 IAM, 리소스 기반 정책 또는 위험 승인과 관련된 변경 사항이 포함됩니다. 이러한 유형의 인시던트는 변경하기 전에 AMS 운영 엔지니어가 RFC를 생성해야 하며 해당 RFC에 대한 승인이 필요합니다. 예를 들어 인시던트 해결에 IAM 정책의 업데이트가 필요한 경우 AMS 보안 검토가 수행되고 AMS 운영 엔지니어가 관리 | 고급 스택 구성 요소 | Identity and Access Management(IAM) | 엔터티 또는 정책 변경 유형 업데이트(ct-27tuth19k52b4)를 사용하여 RFC를 생성하고 진행하기 전에 사용자가 RFC를 승인할 때까지 기다립니다.

Note

이제 AMS는 RFC 승인의 추가 단계 없이 인프라를 변경해야 하는 인시던트 해결을 허용합니다. 인시던트를 해결하는 데 필요한 변경 사항에 보안 검토가 필요하지 않은 경우(변경 사항이 IAM 또는 리소스 기반 정책 또는 위험 승인과 관련이 없음) AMS는 RFC에서 별도의 승인 없이 인시던트에서 받은 승인을 기반으로 변경할 수 있습니다.

인시던트 관리 용어에 대한 정의는 [AMS 주요 용어](#)를 참조하세요.

인시던트의 에스컬레이션 경로를 이해하려면 [도움 받기](#)를 참조하세요.

인시던트에 대한 AMS 대응에 대한 설명은 [AMS 인시던트 대응](#)을 참조하세요.

인시던트 관리란 무엇입니까?

인시던트 관리는 AMS가 활성 인시던트를 기록, 조치, 진행 상황 전달 및 알림을 제공하는 데 사용하는 프로세스입니다.

인시던트 관리 프로세스의 목표는 관리형 서비스의 정상 운영을 최대한 빨리 복원하고, 비즈니스 영향을 최소화하고, 모든 관련 당사자에게 정보를 제공하는 것입니다.

인시던트의 예로는 네트워크 연결의 손실 또는 성능 저하, 응답하지 않는 프로세스 또는 API 또는 예약된 작업이 수행되지 않는 경우(예: 백업 실패) 등이 있습니다(이에 국한되지 않음).

다음 그림은 사용자가 AMS에 보고한 인시던트의 워크플로를 보여줍니다.

이 그래픽은 AMS에서 보고하는 인시던트의 워크플로를 보여줍니다.

인시던트 우선 순위

AWS 지원 센터, 콘솔 또는 지원 API(SAPI)에서 생성된 인시던트는 AMS 콘솔에서 생성된 인시던트와 분류가 다릅니다.

- 낮음: AWS 또는 AMS 리소스와 관련된 비즈니스 서비스 또는 애플리케이션의 중요하지 않은 기능에 영향을 미칩니다.
- 중간: AWS 및/또는 AMS 리소스와 관련된 비즈니스 서비스 또는 애플리케이션이 중간 정도로 영향을 받고 성능이 저하된 상태에서 작동합니다.
- 높음: 비즈니스에 큰 영향을 미칩니다. AWS 및/또는 AMS 리소스와 관련된 애플리케이션의 중요 함수는 사용할 수 없습니다. 프로덕션 시스템에 영향을 미치는 가장 중요한 중단에 대해 예약됩니다.

Note

AWS Support 콘솔은 세 가지 AMS 수준으로 변환되는 다섯 가지 수준의 인시던트 우선 순위를 제공합니다.

문제 대 인시던트

AMS가 인시던트에서 더 큰 결함이나 잘못된 구성이 발견되어 재발할 수 있다고 판단하면 단순한 인시던트가 아닌 문제로 간주됩니다. 이러한 경우 AMS는 문제에 대한 분석을 수행하고 문제 해결을 위한 제안을 제공합니다.

인시던트 관리 서비스 약정

인시던트 관리 서비스 약정

이벤트 또는 작업	서비스 약정 측정
사례 1: 영향이 알려진 이벤트가 생성됩니다. AMS가 인시던트를 열고 알려줍니다.	인시던트 대응 및 인시던트 해결을 위한 클럭은 다음과 같은 경우에 시작됩니다.
사례 2: AMS가 사용자에게 연락하여 이벤트의 영향을 확인합니다. 이벤트가 인시던트인지 확인합니다.	사례 1: AMS가 인시던트를 생성합니다. 사례 2: 알림이 인시던트임을 확인합니다.

이벤트 또는 작업	서비스 약정 측정
사례 3: 문제를 발견하고 인시던트 보고서를 제출합니다.	사례 3: 인시던트를 제출합니다. 서비스 약정은 생성된 인시던트의 우선 순위에 따라 달라집니다.
인시던트를 제출하면 AMS가 응답을 전송하여 인시던트를 승인합니다. AMS가 사용자를 대신하여 인시던트를 생성하는 경우 별도의 인시던트 응답이 전송되지 않습니다.	인시던트 해결을 위한 클럭은 계속됩니다. AMS가 인시던트 승인을 보내면 인시던트 대응 시간에 대한 클럭이 중지됩니다.  Note 사용자의 입력을 기다리는 데 소요된 시간은 인시던트 해결 시간 계산에서 제외됩니다. AMS가 생성하는 인시던트의 경우 초기 응답 시간은 초기 인시던트 알림을 생성한 시간입니다.

이벤트 또는 작업	서비스 약정 측정
해당 리소스/서비스의 경우 AMS는 상태를 확인하여 다음 사항을 확인합니다. - AMS에서 감지한 이벤트 또는 고객이 제출한 인시던트는 인시던트로 간주됩니다. - 인시던트의 우선 순위가 올바른 경우 제출하는 인시던트의 우선 순위가 올바르지 않은 경우 AMS는 인시던트의 우선 순위를 다시 지정합니다. AMS가 인시던트 우선 순위를 변경하면 우선 순위 변경의 근거와 함께 알림이 전송됩니다. 경우에 따라 제출한 문제가 원인에 따라 인시던트로 간주되지 않을 수 있습니다. 이러한 경우 AMS는 인시던트를 종료하고 이유를 설명하는 알림을 보냅니다. 이벤트 분류와 관계없이 AMS는 사용자와 협력하여 필요에 따라 지원합니다. 인시던트 분류 규칙을 이해하려면 섹션을 참조하세요 인시던트 우선 순위.	인시던트 우선 순위가 변경되는 경우 새 우선 순위에 대한 서비스 약정이 적용됩니다. 클럭은 계속 표시됩니다. 인시던트 정의에 부합하지 않아 인시던트가 종료된 경우 서비스 약정이 적용되지 않으며 클럭이 중지됩니다.
AMS는 인시던트를 서비스 약정 내에서 해결하기 위해 작업합니다. 경우에 따라 AMS가 사용할 수 없는 스택(들) 또는 리소스(들)를 적시에 해결할 수 없다고 판단하면 AMS는 인프라 복원을 해결 옵션으로 제공합니다. 인프라 복원에는 사용자가 달리 지정하지 않는 한 영향을 받는 스택(들)의 템플릿을 기반으로 기존 스택(들)을 재배포하고 마지막으로 알려진 복원 지점(EBS/RDS 스냅샷)을 기반으로 데이터 복원을 시작하는 작업이 포함됩니다. 개별 EC2 인스턴스의 임시 데이터는 손실됩니다. AWS에서 권장하는 대로 인프라 복원을 승인하지 않으면 연결된 인시던트 해결 시간 서비스 약정에 대한 서비스 크레딧을 받을 수 없습니다.	다음과 같은 경우 시계가 중지됩니다. - AMS가 해당 인시던트와 관련된 모든 사용 불가 서비스 또는 리소스를 사용 가능한 상태로 복원한 경우 - 인프라 복원이 시작됩니다.

이벤트 또는 작업	서비스 약정 측정
경우에 따라 사전 정의되고 승인된 작업이 없는 한 인시던트 해결 작업을 계속 진행하기 위해 AMS에서 사용자의 설명 또는 활동이 필요합니다. 따라서 인시던트를 해결하기 위해 AMS와 사용자 간에 통신이 이루어집니다.	AMS가 사용자의 응답 또는 작업을 기다리고 있는 경우 클록이 중지됩니다. AMS가 사용자로부터 응답을 받거나 AMS가 사용자에게 요구하는 작업이 완료되면 클록이 다시 시작됩니다.

Note

서비스 약정의 전체 목록을 보려면 [AMS 서비스 수준 계약을](#) 다운로드하세요.

인시던트 관리 예제

인시던트 관리 예제입니다.

주제

- [인시던트 테스트](#)
- [인시던트 보고](#)
- [인시던트 모니터링 및 업데이트](#)
- [AWS Support API를 사용하여 인시던트 관리](#)
- [AMS 생성 인시던트에 대응](#)

다음 예제에서는 AMS 콘솔을 사용하여 인시던트를 제출하는 방법을 설명합니다. 제출되면 AMS 팀은 고객과 협력하여 서비스 수준 계약(SLA)에 따라 인시던트를 해결합니다.

인시던트 테스트

AMS 인시던트 제출을 테스트할 때 제목 텍스트에 AMSTestNoOpsActionRequired 플래그를 포함해야 합니다. 이 플래그는 인시던트 제출이 테스트용임을 AMS에 알립니다. AMS 운영 엔지니어는 해당 플래그를 확인하면 인시던트 제출에 어떤 식으로든 응답하지 않습니다.

인시던트 보고

AMS 콘솔을 사용하여 인시던트를 보고합니다. 각 새 문제 또는 질문에 대해 새 인시던트를 생성하는 것이 중요합니다. 이전 문의와 관련된 사례를 개설할 때는 이전 서신을 참조할 수 있도록 관련 사례 번호를 포함하는 것이 좋습니다.

Note

사례 대응 서신이 원래 문제에서 벗어나는 경우 AMS 운영자가 새 인시던트를 보고하도록 요청할 수 있습니다.

AMS 콘솔을 사용하여 인시던트를 보고하려면:

1. 왼쪽 탐색 창에서 인시던트를 선택합니다.

인시던트 목록이 열립니다.

인시던트 목록이 비어 있는 경우 필터 지우기 옵션은 필터를 모든 상태로 재설정합니다.

전화 또는 채팅을 사용하려는 경우 지원 센터에서 인시던트 생성을 클릭하여 AMS 서비스 유형으로 자동 채워진 지원 센터 콘솔에서 인시던트 생성 페이지를 엽니다.

Important

- 를 사용하여 시작된 전화 통화가 녹음 지원 되어 응답을 개선할 수 있습니다. 통화가 끊어지면 지원 센터 사례를 통해 다시 호출해야 합니다. AWS에는 다시 호출하는 메커니즘이 없습니다.
- 전화 및 채팅 지원은 RFC 또는 보안 문제가 아닌 지원 사례, 인시던트 및 서비스 요청에 도움이 되도록 설계되었습니다.
- RFC 문제의 경우 관련 RFC 세부 정보 페이지의 대응 옵션을 사용하여 AMS 엔지니어에게 문의하세요.
- 보안 문제의 경우 우선 순위가 높은(P1 또는 P2) 지원 사례를 생성합니다. 실시간 채팅 기능은 보안 이벤트용이 아닙니다.

2. 기존 인시던트를 찾으려면 드롭다운 목록에서 인시던트 상태 필터를 선택합니다.

- 아직 해결되지 않은 모든 인시던트입니다.
- 아직 할당되지 않은 새 인시던트입니다.
- 할당된 인시던트입니다.
- 다시 연 인시던트입니다.
- 할당되고 복잡한 인시던트입니다.
- 다음 단계 전에 피드백이 필요한 인시던트입니다.
- 최근에 정보를 제출한 인시던트입니다.
- 종료된 인시던트입니다.
- 계정의 모든 인시던트입니다.

3. 생성(Create)을 선택합니다.

인시던트 생성 페이지가 열립니다.

4. 우선 순위를 선택합니다.

- 낮음: AWS/AMS 리소스와 관련된 비즈니스 서비스 또는 애플리케이션의 중요하지 않은 기능에 영향을 미칩니다.
- 중간: AWS/AMS 리소스와 관련된 비즈니스 서비스 또는 애플리케이션은 중간 정도로 영향을 받고 성능이 저하된 상태에서 작동합니다.
- 높음: 비즈니스에 큰 영향을 미칩니다. AWS/AMS 리소스와 관련된 애플리케이션의 중요 함수는 사용할 수 없습니다. 프로덕션 시스템에 영향을 미치는 가장 중요한 중단에 대해 예약됩니다.

5. 범주를 선택합니다.

Note

인시던트 기능을 테스트하려는 경우 인시던트 제목에 무작업 플래그 (AMSTestNoOpsActionRequired)를 추가합니다.

6. 다음에 대한 정보를 입력합니다.

- 제목: 인시던트 보고서의 설명 제목입니다.

- CC 이메일: 인시던트 보고서 및 해결 방법에 대한 정보를 제공하려는 사람의 이메일 주소 목록입니다.
- 세부 정보: 인시던트, 영향을 받는 시스템 및 해결의 예상 결과에 대한 포괄적인 설명입니다. 미리 설정된 질문에 답변하거나 삭제하고 관련 정보를 입력합니다.

첨부 파일을 추가하려면 첨부 파일 추가를 선택하고 원하는 첨부 파일로 이동한 다음 열기를 클릭합니다. 첨부 파일을 삭제하려면 삭제 아이콘을 클릭합니다

7. 제출을 선택합니다.

유형, 제목, 생성됨, ID, 상태 등 인시던트에 대한 정보와 생성한 요청에 대한 설명이 포함된 서신 영역이 포함된 세부 정보 페이지가 열립니다.

회신을 클릭하여 대응 영역을 열고 상태에 추가 세부 정보 또는 업데이트를 제공합니다.

인시던트가 해결되면 사례 종료를 클릭합니다.

한 페이지에 맞는 것보다 더 많은 서신이 있는 경우 더 로드를 클릭합니다.

커뮤니케이션을 평가하는 것을 잊지 마세요!

인시던트가 인시던트 목록 페이지에 표시됩니다.

YouTube 동영상: [AWS Managed Services 콘솔에서 인시던트를 제기하려면 어떻게 해야 하나요?](#)

인시던트 모니터링 및 업데이트

사례라고 하는 인시던트 보고서 및 서비스 요청을 AMS 콘솔을 사용하거나 지원 API를 사용하여 프로그래밍 방식으로 업데이트, 모니터링 및 검토할 수 있습니다. 지원 API 사용에 대한 자세한 내용은 [DescribeCases](#) 작업을 참조하세요.

AMS 콘솔을 사용하여 사례, 인시던트 또는 서비스 요청을 모니터링하려면 다음 단계를 따릅니다.

1. AMS 콘솔 인시던트 보고서 또는 서비스 요청 대시보드에서 사례로 이동하여 제목을 선택하여 현재 상태 및 서신이 포함된 세부 정보 페이지를 엽니다.

AMS 운영 팀에서 보고된 인시던트 또는 서비스 요청 사례를 업데이트하면 응답할 수 있도록 AMS 콘솔에서 인시던트에 대한 이메일과 링크를 받게 됩니다. 이메일에 회신하여 인시던트 대응 서신에 응답할 수 없습니다.

Important

서비스 요청 또는 인시던트 사례에 대한 상태 변경 알림을 받으려면 이메일 주소를 입력해야 합니다. 알림은 생성 시 사례에 추가된 이메일 주소로만 전송됩니다.

AMS 페더레이션 네트워크에서 이메일 서버를 사용하지 않는 한 알림 이메일의 링크는 작동하지 않습니다. 그러나 AMS 콘솔로 이동하여 사례 세부 정보 페이지를 사용하여 서신에 응답할 수 있습니다.

2. 목록에 사례가 많은 경우 필터 옵션을 사용할 수 있습니다.
 - 모두 열기(기본값): 이 필터를 사용하여 해결되지 않은 모든 사례를 확인합니다.
 - 할당되지 않음: 사례를 방금 제출했고 사례 상태가 변경되었다는 알림을 받지 못한 경우 사용합니다. 인시던트 및 서비스 요청 사례는 제출된 우선 순위(인시던트) 또는 서비스 수준 계약(서비스 요청)에 따라 다른 프롬프트로 처리됩니다.
 - 열기: 사례가 "Amazon 보류 중" 작업이라는 알림을 받은 경우 사용합니다. 이는 사례가 할당되었지만 작업이 아직 시작되지 않았음을 의미합니다.
 - 다시 열기: 해결된 후 사례가 다시 열렸다는 알림을 받은 경우 사용합니다.
 - 작업 진행 중: 운영자가 사례 작업을 시작했다는 알림을 받은 경우를 사용합니다.
 - 대기 중인 고객 작업: 사용자 측 작업에 대한 운영자 요청을 받은 경우를 사용합니다.
 - 고객 작업 완료: 사례에 대한 작업이 처리되었다는 알림을 받은 경우를 사용합니다.
 - 해결됨: 해결된 것으로 알려진 사례를 보는 데 사용합니다. 해결된 사례는 12개월 동안 기록으로 유지됩니다.
 - 모든 상태: 상태에 관계없이 모든 사례를 보려면 이 필터를 사용합니다.
3. 최신 상태를 확인하려면 페이지를 새로 고칩니다.
4. 모든 서신이 페이지에 표시되지 않는 서신이 너무 많으면 더 보기를 선택합니다.
5. 사례 상태를 업데이트하려면 회신을 선택하고 새 서신을 입력한 다음 제출을 선택합니다.
6. 만족스럽게 해결된 후 사례를 종료하려면 사례 종료를 선택합니다.

AMS에 진행 상황을 알리려면 1~5점 평점을 통해 서비스를 평가해야 합니다.

AWS Support API를 사용하여 인시던트 관리

[AWS Support API](#)를 사용하면 문제 조사 및 AWS Support 직원과의 상호 작용 전반에 걸쳐 인시던트를 생성하고 인시던트에 대응 서신을 추가할 수 있습니다. AWS Support API는 [AWS Support Center](#)의 대부분의 동작을 모델링합니다. 이 AWS 지원 서비스를 사용하는 방법에 대한 자세한 내용은 [AWS 지원 사례 프로그래밍](#)을 참조하세요.

Note

AWS Support API 또는 SAPI를 AMS Advanced 인시던트에 사용할 때는 서비스 코드를 사용합니다 `sentinel-report-incident`.

AMS 생성 인시던트에 대응

AMS는 리소스를 사전에 모니터링합니다. 자세한 내용은 [모니터링 및 이벤트 관리](#)를 참조하세요. AMS가 인시던트를 식별하고 생성하는 경우가 있으며, 가장 자주 인시던트를 알립니다. 인시던트를 해결하기 위해 조치가 필요한 경우 AMS는 계정에 제공한 연락처 정보로 알림을 보냅니다. 다른 인시던트와 동일한 방식으로 이 인시던트에 대응합니다. 일반적으로 AMS 콘솔을 통해 인시던트에 대응합니다. 경우에 따라 이메일 또는 전화로 문의해야 합니다.

Note

AMS는 AWS 계정의 기본 이메일 주소로 통신을 전송합니다. 인시던트 관리 프로세스를 용이하게 하기 위해 대체 운영 연락처 이메일 별칭을 추가하는 것이 좋습니다. 이는 AMS 온보딩 프로세스 및 관련 온보딩 설명서에서 다룹니다. 온보딩 중에 리소스 기반이 아닌 연락처(CSDM에 알린 연락처)를 AMS에 제공한 경우 해당 연락처가 사용됩니다. 예를 들어 보안 관련 인시던트 또는 알림에 사용할 "SecurityContacts"라는 연락처 목록을 CSDMs/CAs에 제공할 수 있습니다. 태그 정보 사용에 대해 CSDM에 동의한 경우 인스턴스/리소스의 연락처 태그는 AMS 생성 인시던트에 사용됩니다.

이 알림 서비스에 대한 자세한 내용은 [알림](#)을 참조하세요.

서비스 요청 관리

주제

- [서비스 요청을 사용해야 하는 경우](#)
- [서비스 요청 관리 작동 방식](#)

- [AMS에서 서비스 요청 테스트](#)
- [AMS에서 서비스 요청 생성](#)
- [AMS에서 서비스 요청 모니터링 및 업데이트](#)
- [AMS 생성 서비스 요청에 응답](#)

서비스 요청은 사용자가 정보 또는 조언을 요청하기 위해 생성한 AMS와의 통신입니다. 표준 서비스 요청의 좋은 예는 경보 관리자, 패치 오케스트레이터 등과 같은 AMS 서비스를 구성하는 데 도움이 되거나 지침을 제공하는 것입니다. AMS로부터 서비스 요청을 받을 수도 있습니다. 이를 아웃바운드 서비스 요청 또는 서비스 알림이라고 합니다. AMS에서 전송한 서비스 요청 및 아웃바운드 서비스 요청(서비스 알림) 목록을 보려면 AMS 콘솔의 서비스 요청 페이지를 참조하세요.

아웃바운드 서비스 요청에 대한 자세한 내용은 섹션을 참조하세요 [AMS 생성 서비스 요청에 응답](#).

AMS 콘솔을 사용하거나 프로그래밍 방식으로 지원 API를 사용하여 AWS Managed Services(AMS) 서비스 요청을 생성합니다. API 사용에 대한 자세한 내용은 [지원 API](#)를 참조하세요. AMS에서 `sentinel-service-request` 서비스 코드를 선택합니다.

AMS 운영 팀이 서비스 요청을 수신하면 서비스 수준 계약에 따라 우선 순위가 지정됩니다. 서비스 요청 해결 프로세스의 각 단계에서 정보를 받으려면 CC 이메일 옵션을 채우고 페더레이션으로 연결하는 경우 AMS가 보내는 이메일의 링크를 따라가기 전에 로그인해야 합니다.

AMS 콘솔 서비스 요청 생성 페이지를 사용하여 다음 작업을 수행합니다.

- 서비스 요청 생성 및 업데이트
- 모든 현재 서비스 요청의 목록 및 세부 정보 가져오기
- 해결된 요청을 포함하여 날짜 및 인시던트 식별자별로 서비스 요청 검색 범위를 좁힙니다.
- 요청에 커뮤니케이션 및 파일 첨부 파일을 추가하고 사례 대응을 위해 이메일 수신자를 추가합니다.
- 서비스 요청 해결
- 서비스 요청 커뮤니케이션 평가

서비스 요청을 사용해야 하는 경우

다음 예제에서는 서비스 요청을 설명합니다.

- AMS 또는 AWS 일반 지침
- 패치 MW 관련 질문

- 백업 일정 관련 질문
- AWS 서비스 기능에 대한 질문

다음은 서비스 요청에서 발생해서는 안 되는 사항의 예입니다.

- 액세스 문제
- 패치 실패
- 백업 실패
- RFC 장애 또는 비즈니스 종단을 유발하는 RFC(비즈니스 종단에 인시던트 사용)
- RFC 질문 또는 RFC 범위의 추가 입력 또는 변경(RFC 양방향 대응 사용)

서비스 요청 관리 작동 방식

서비스 요청은 대기 중인 AMS 운영 팀에서 처리합니다.

AMS 운영 팀에서 서비스 요청을 수신한 후에는 요청이 인시던트로 더 적절하게 분류되지 않도록 검토됩니다. 인시던트로 분류해야 하는 경우 즉시 재분류되고 AMS 인시던트 관리 팀이 인계하며 알림을 받습니다.

RFC 제출로 서비스 요청을 해결할 수 있는 경우 검토 운영자는 적절한 RFC 제출을 요청하는 이메일을 보냅니다(자세한 내용은 제공됨).

AMS 운영자가 서비스 요청을 해결할 수 있는 경우 이를 위한 단계가 즉시 수행됩니다. 예를 들어 서비스 요청이 아키텍처 조언 또는 기타 정보용인 경우 운영자는 적절한 리소스를 참조하거나 질문에 직접 답변합니다.

서비스 요청 분석에서 버그 또는 기능 요청이 식별되면 AMS는 서비스 요청을 통해 알림을 보냅니다. 기능 요청 또는 버그 수정에 대한 ETA가 없으므로 원래 서비스 요청이 종료됩니다. 원래 서비스 요청과 관련된 후속 질문은 CSDM에 문의하십시오.

서비스 요청이 AMS 작업 범위를 벗어나는 경우 운영자는 진행 중인 단계에 대한 이메일과 함께 사용자 또는 적절한 AWS 운영 팀과 통신할 수 있도록 클라우드 서비스 제공 관리자에게 요청을 보냅니다.

결과에 만족한다고 표시할 때까지 서비스 요청은 해결되지 않습니다.

Note

원활한 커뮤니케이션을 위해 모든 경우에 연락처 이메일, 이름 및 전화번호를 제공하는 것이 좋습니다.

AMS에서 서비스 요청 테스트

AMS 서비스 요청을 테스트할 때 제목 텍스트에 AMSTestNoOpsActionRequired 플래그를 포함하여 AMS에 서비스 요청이 테스트용임을 알리도록 요청합니다. AMS 작업 엔지니어는 해당 플래그를 확인하면 서비스 요청에 응답하지 않습니다.

AMS에서 서비스 요청 생성

AWS Managed Services(AMS) 콘솔을 사용하여 서비스 요청을 생성하려면:

1. 왼쪽 탐색에서 서비스 요청을 선택합니다.

서비스 요청 목록이 열립니다.

서비스 요청 목록이 비어 있는 경우 필터 지우기 옵션은 필터를 모든 상태로 재설정합니다.

전화 또는 채팅을 사용하려는 경우 지원 센터에서 서비스 요청 생성을 클릭하여 AMS 서비스 유형으로 자동 채워진 지원 센터 콘솔에서 서비스 요청 생성 페이지를 엽니다.

Note

지원 중앙에서 시작된 전화 통화는 응답을 더 잘 개선하기 위해 녹음됩니다. 호출이 끊어지면 지원 센터 사례를 통해 다시 호출해야 합니다. AWS에는 다시 호출하는 메커니즘이 없습니다.

⚠ Important

전화 및 채팅 지원은 지원 사례, 인시던트 및 서비스 요청에 도움이 되도록 설계되었습니다. RFC 문제의 경우 관련 RFC 세부 정보 페이지의 대응 옵션을 사용하여 AMS 엔지니어에게 문의하세요.

2. 기존 서비스 요청을 찾으려면 드롭다운 목록에서 서비스 요청 상태 필터를 선택합니다.

- 아직 해결되지 않은 모든 서비스 요청입니다.
- 아직 할당되지 않은 새 서비스 요청입니다.
- 할당된 서비스 요청입니다.
- 다시 연 서비스 요청입니다.
- 할당되고 복잡한 서비스 요청입니다.
- 다음 단계 전에 피드백이 필요한 서비스 요청입니다.
- 최근에 정보를 제출한 서비스 요청입니다.
- 가 종료한 서비스 요청입니다.
- 계정의 모든 서비스 요청입니다.

3. 생성(Create)을 선택합니다.

서비스 요청 생성 페이지가 열립니다.

4. 범주를 선택합니다.

i Note

서비스 요청 기능을 테스트하려면 서비스 요청 제목에 무작업 플래그 `AMSTestNoOpsActionRequired`를 추가합니다.

5. 다음에 대한 정보를 입력합니다.

- 제목: 그러면 목록 페이지에 서비스 요청 세부 정보에 대한 링크가 생성됩니다.

- CC 이메일: 이러한 이메일은 기본 이메일 연락처 외에도 서신을 수신합니다.
- 세부 정보: 여기에 최대한 많은 정보를 제공합니다.

첨부 파일을 추가하려면 첨부 파일 추가를 선택하고 원하는 첨부 파일로 이동한 다음 열기를 클릭합니다. 첨부 파일을 삭제하려면 삭제 아이콘을 클릭합니다.

6. 제출을 선택합니다.

유형, 주체, 생성됨, ID, 상태 등 서비스 요청에 대한 정보와 생성한 요청에 대한 설명이 포함된 서신 영역이 포함된 세부 정보 페이지가 열립니다.

또한 서비스 요청은 서비스 요청 목록 페이지에 표시됩니다. 알림이 있지만 아직 AMS에서 듣지 않은 경우이 옵션을 사용합니다.

회신을 클릭하여 대응 영역을 열고 추가 세부 정보 또는 상태 업데이트를 제공합니다.

서비스 요청이 해결되면 사례 해결을 클릭합니다.

더 보기를 클릭하여 초기 페이지에 맞지 않는 추가 서신을 봅니다.

커뮤니케이션을 평가하는 것을 잊지 마세요!

결제 관련 쿼리의 경우 지원 센터 콘솔에서 서비스 요청 사례를 생성합니다.

YouTube 동영상: [AWS 콘솔에서 서비스 요청을 제기하는 방법 및 시기와 서비스 수준 목표란 무엇입니까?](#)

AMS에서 서비스 요청 모니터링 및 업데이트

사례라고 하는 인시던트 보고서 및 서비스 요청을 AMS 콘솔을 사용하거나 지원 API를 사용하여 프로그래밍 방식으로 업데이트, 모니터링 및 검토할 수 있습니다. 지원 API 사용에 대한 자세한 내용은 [DescribeCases](#) 작업을 참조하세요.

AMS 콘솔을 사용하여 사례, 인시던트 또는 서비스 요청을 모니터링하려면 다음 단계를 따릅니다.

1. AMS 콘솔 인시던트 보고서 또는 서비스 요청 대시보드에서 사례로 이동하여 제목을 선택하여 현재 상태 및 서신이 포함된 세부 정보 페이지를 엽니다.

AMS 운영 팀에서 보고된 인시던트 또는 서비스 요청 사례를 업데이트하면 응답할 수 있도록 AMS 콘솔에서 인시던트에 대한 이메일과 링크를 받게 됩니다. 이메일에 회신하여 인시던트 대응에 응답할 수 없습니다.

 Important

서비스 요청 또는 인시던트 사례에 대한 상태 변경 알림을 받으려면 이메일 주소를 입력해야 합니다. 알림은 생성 시 사례에 추가된 이메일 주소로만 전송됩니다.

AMS 페더레이션 네트워크에서 이메일 서버를 사용하지 않으면 알림 이메일의 링크가 작동하지 않습니다. 그러나 AMS 콘솔로 이동하여 사례 세부 정보 페이지를 사용하여 서신에 응답할 수 있습니다.

2. 목록에 사례가 많은 경우 필터 옵션을 사용할 수 있습니다.
 - 모두 열기(기본값): 이 필터를 사용하여 해결되지 않은 모든 사례를 확인합니다.
 - 할당되지 않음: 사례를 방금 제출했지만 사례 상태가 변경되었다는 알림을 받지 못한 경우 사용합니다. 인시던트 및 서비스 요청 사례는 제출된 우선순위(인시던트) 또는 서비스 수준 계약(서비스 요청)에 따라 다른 프롬프트로 처리됩니다.
 - 열기: 사례가 "Amazon 보류 중" 작업이라는 알림을 받은 경우 사용합니다. 이는 사례가 할당되었지만 작업이 아직 시작되지 않았음을 의미합니다.
 - 다시 열기: 해결된 후 사례가 다시 열렸다는 알림을 받은 경우 사용합니다.
 - 작업 진행 중: 운영자가 사례 작업을 시작했다는 알림을 받은 경우를 사용합니다.
 - 대기 중인 고객 작업: 사용자 측 작업에 대한 운영자 요청을 받은 경우를 사용합니다.
 - 고객 작업 완료: 사례에 대한 작업이 처리되었다는 알림을 받은 경우를 사용합니다.
 - 해결됨: 해결된 것으로 알려진 사례를 보는 데 사용합니다. 해결된 사례는 12개월 동안 기록으로 유지됩니다.
 - 모든 상태: 상태에 관계없이 모든 사례를 보려면 이 필터를 사용합니다.
3. 최신 상태를 확인하려면 페이지를 새로 고칩니다.
4. 모든 서신이 페이지에 표시되지 않는 서신이 너무 많으면 더 보기를 선택합니다.
5. 사례 상태를 업데이트하려면 회신을 선택하고 새 서신을 입력한 다음 제출을 선택합니다.
6. 만족스럽게 해결된 후 사례를 종료하려면 사례 종료를 선택합니다.

별점 1~5점을 통해 서비스를 평가하여 AMS에 진행 상황을 알려야 합니다.

AMS 생성 서비스 요청에 응답

AMS 패치 관리는 설정된 유지 관리 기간 이전에 서비스 요청(서비스 알림)을 전송합니다. 자세한 내용은 [AMS 유지 관리 기간](#)을 참조하세요. 또한 AMS는 인프라가 서비스의 영향을 받을 가능성이 있거나 계정의 EC2 인스턴스를 재부팅해야 할 수 있는 경우 AWS 서비스 알림을 전송합니다. 자세한 내용은 [서비스 알림](#)을 참조하세요.

Note

AMS는 사용자가 제공한 AWS 계정의 기본 이메일 주소로 통신을 전송합니다. 서비스 요청 또는 서비스 알림 관리 프로세스를 용이하게 하기 위해 대체 운영 연락처 이메일 별칭을 추가하는 것이 좋습니다. 이러한 이메일 추가는 AMS 온보딩 프로세스 및 관련 온보딩 설명서에서 다룹니다.

결제 질문

결제 관련 질문을 제출하려면 다음 단계를 완료하세요.

1. <https://console.aws.amazon.com/support/home> [AWS Support 센터](#)를 엽니다.
2. 계정 및 결제를 선택합니다.
3. 사례 생성을 선택합니다.
4. 계정 및 결제를 선택한 다음 프롬프트에 따라 사례를 제출합니다.

온디맨드 작업

OOD(Otions on Demand)는 현재 AMS 운영 계획 또는에서 기본적으로 제공하지 않는 운영 서비스를 제공하여 AMS 운영 계획의 표준 범위를 확장하는 AWS Managed Services(AMS) 기능입니다 AWS. <https://aws.amazon.com/managed-services/features/> 선택하면 자동화와 고도로 숙련된 AMS 리소스의 조합으로 카탈로그 오퍼링이 제공됩니다. 장기 약정이나 추가 계약이 없으므로 필요에 따라 기존 AMS와 AWS 운영 및 기능을 확장할 수 있습니다. 사용자는 매월 블록당 20시간의 시간 블록(OOD 블록)을 구매하는 데 동의합니다.

표준화된 상품 카탈로그에서 선택하고 서비스 요청을 통해 새 OOD 참여를 시작할 수 있습니다. OOD 상품의 예로는 Amazon EKS 유지 관리, SAP 클러스터 운영 AWS Control Tower 및 관리 지원이 있습니다. 새로운 카탈로그 상품은 수요와 가장 자주 볼 수 있는 운영 사용 사례에 따라 정기적으로 추가됩니다.

OOD는 AMS Advanced 및 AMS Accelerate 운영 플랜 모두에 사용할 수 있으며 AMS를 사용할 수 [AWS 리전](#) 있는 모든에서 사용할 수 있습니다.

AMS는 요청된 변경 사항을 구현하는 동안 고객 보안 위험 관리(CSRM)를 수행합니다. CSRM 프로세스에 대한 자세한 내용은 [변경 요청 보안 검토](#)를 참조하세요.

오퍼링의 온디맨드 작업 카탈로그

OOD(Otions on Demand)는 다음 표에 설명된 서비스를 제공합니다.

Note

주요 용어의 정의는 AWS Managed Services 설명서 [주요 용어](#)를 참조하세요.

운영 계획	제목	설명	예상 결과
AMS Accelerate	Amazon EKS 클러스터 유지 관리	AMS는 Amazon Elastic Kubernetes Service(Amazon EKS) 배포의 지속적인 유지 관리를 처리하여 컨테이너 개발자를 확보합니다. AMS는 컨트롤 플레인, 추가 기능 및 노드의 구성 요소를 처리하는 클러스터를 업데이트하는 데 필요한 end-to-en	고객 팀은 Amazon EKS 클러스터 업데이트의 기본 작업을 지원했습니다.

		d 절차를 수행합니다. AMS는 관리형 노드 유형과 큐레이션된 Amazon EKS 및 Kubernetes 추가 기능에 대한 업데이트를 수행합니다.	
AMS Accelerate	AMI 구축 및 판매	AMS는 고객을 위한 AMI 구축 및 판매를 지속적으로 관리합니다. 엔지니어는 구독한 AMIs의 월간 릴리스를 수행하고, 긴급 패치 작업에 대한 온디맨드 AMIs를 릴리스하고, 실행서를 사용하여 변경 사항을 관리하고, CloudWatch Monitoring을 사용하여 AMI 빌드를 모니터링합니다. 또한 지정된 계정에 사용되는 모든 AMIs에 대한 문제 해결 지원 및 자세한 보고를 제공합니다. 이 서비스를 사용하려면 EC2 이미지 빌더를 통해 AMI 빌드 파이프라인을 배포해야 합니다. AMS는 EC2 Image 빌더와 상호 작용하는 다른 자동화 또는 서비스를 지원하지 않습니다.	고객 보안 태세가 개선되고 AMIs 단축되었습니다.

AMS Accelerate	큐레이션된 변경 실행	숙련된 운영 엔지니어와 협력하여 비즈니스 요구 사항을 AWS 환경 내에서 안전하게 실행할 수 있는 검증된 변경 요청으로 변환합니다. 자동화에 대한 고유한 접근 방식과 운영 모범 사례(예: 영향 평가, 롤백, 2인 규칙)에 대한 지식을 활용합니다. 이는 규모에 따른 간단한 변경이든 다운스트림 영향이 있는 복잡한 작업이든 상관없습니다.	고객은 사용자 지정 변경 요청의 정의, 생성 및 실행을 지원했습니다. 변경 사항은 수동 또는 자동(CloudFormation, SSM)일 수 있습니다. 필요한 경우 구성 지침에 지원 대한와의 상담을 포함합니다. 애플리케이션 코드, 애플리케이션 설치/배포, 데이터 마이그레이션 또는 OS 구성 변경을 위한 것이 아닙니다.
AMS Accelerate	AWS Network Firewall 운영	AMS는 사용자와 협력하여 방화벽을 온보딩하고 지속적인 방화벽 작업에 대한 정책 및 규칙을 구현하고 관리합니다. 엔지니어는 운영 모범 사례와 자동화를 활용하여 표준화된 정책 및 규칙을 구성하고 모니터링을 활성화하여 자동화 프로세스 외부에서 이루어진 변경 사항을 감지함으로써 이를 수행합니다. AMS는 원치 않는 변경 사항을 신속하게 알리고 요청 시 이를 포함하거나 이전 구성으로 계정을 복원하여 시스템의 전반적인 안정성을 보장하는 옵션을 제공합니다.	고객 팀은 의도하지 않은 네트워크 방화벽 변경을 신속하게 감지하여 관리 오버헤드를 줄이는 데 도움을 주었으며, 이로 인해 인시던트 해결이 개선되고 예상 및 예상치 못한 문제에 대한 근본 원인 분석 시간이 단축되었습니다.

AMS Accelerate	AWS Control Tower 작업	AWS Transit Gateway 및를 포함한 AWS Control Tower 랜딩 존의 지속적인 운영 및 관리 AWS Organizations - 포괄적인 랜딩 존 솔루션을 제공합니다. 사용자 지정 제어 및 가드레일 라이브러리를 사용하여 계정 벤딩, SCP 및 OU 관리, 드리프트 수정, SSO 사용자 관리 및 AWS Control Tower 업그레이드를 처리합니다.	고객 팀은 일부 기본 운영 작업인 AWS Control Tower, AWS Transit Gateway 및를 지원했습니다 AWS Organizations.
AMS Accelerate	AWS 랜딩 존 Accelerate 작업	AMS는 AWS Landing Zone Accelerator(LZA)를 통해 배포된 AWS 랜딩 존의 지속적인 작업을 제공합니다. 엔지니어는 구성 파일 변경, AWS Control Tower (CT) 환경 관리(계정 벤딩, OU 생성, CT 가드레일), 서비스 제어 정책(SCP) 관리, CT 드리프트 감지 및 수정, 네트워크 구성 관리, CT 및 LZA 프레임워크 업데이트 등을 처리합니다. AWS LZA는와 같은 운영 모범 사례와 서비스를 사용하여 안전한 다중 계정 AWS 환경을 설정하고 관리할 수 있는 수단을 제공합니다 AWS Control Tower.	고객 팀은 AWS Landing Zone Accelerator 솔루션의 지속적인 운영 및 관리를 지원했습니다.
AMS Accelerate	SAP 클러스터 지원	SAP 클러스터에 대한 전용 경보, 모니터링, 클러스터 패치 적용, 백업 및 인시던트 수정. 이 카탈로그 항목을 사용하면 SAP 운영 팀에서 진행 중인 운영 작업 중 일부를 오프로드하여 용량 관리 및 성능 튜닝에 집중할 수 있습니다.	고객 또는 파트너 SAP 팀이 일부 기본 작업을 지원했습니다. 여전히 고객은 용량 관리, 성능 튜닝, DBA 및 SAP 기본 관리와 같은 다른 SAP 기능을 제공해야 합니다.

AMS Accelerate	EC2 작업의 SQL Server	AMS는 사용자와 협력하여 EC2 인스턴스에 배포된 SQL Server 데이터베이스의 지속적인 작업을 온보딩, 구현 및 관리합니다. 엔지니어는 운영 모범 사례와 자동화를 활용하여 백업 및 패치와 같은 작업을 수행하고, 클러스터 인식 롤링 업데이트를 포함하도록 AMS 운영 지원을 SQL Server 패치로 확장하고, 랜섬웨어 방어 전략에 맞는 백업 및 복원 서비스를 포함하고, 고객이 제공한 백업 및 패치 제어 준수를 모니터링하여 데이터베이스 팀을 확보합니다.	SQL Server 고객은 자체 라이선스(BYOL)를 EC2로 가져와 라이선스 비용을 최적화하는 것 외에도 패치 및 백업 데이터베이스 작업을 오프로드하여 워크로드의 복원력과 보안 태세를 개선하도록 지원했습니다.
AMS 고급	Amazon EKS 클러스터 유지 관리	AMS는 Amazon Elastic Kubernetes Service(Amazon EKS) 배포의 지속적인 유지 관리 및 상태를 처리하여 컨테이너 개발자를 확보합니다. AMS는 컨트롤 플레인, 추가 기능 및 노드의 구성 요소를 처리하는 클러스터를 업데이트하는 데 필요한 end-to-end 절차를 수행합니다. AMS는 관리형 노드 유형과 큐레이션된 Amazon EKS 및 Kubernetes 추가 기능에 대한 업데이트를 수행합니다.	고객 팀은 Amazon EKS 클러스터 업데이트의 기본 작업을 지원했습니다.
AMS 고급	우선 순위 RFC 실행	지정된 AMS 운영 엔지니어 용량은 변경 요청(RFC) 실행의 우선순위를 정합니다. 모든 제출은 더 높은 수준의 응답을 받으며 Amazon Chime 회의실을 통해 엔지니어와 직접 상호 작용하여 우선 순위 순서를 조정할 수 있습니다.	고객은 RFCs에 대해 8시간의 응답 SLO를 받습니다.

AMS Advanced 및 AMS Accelerate	레거시 OS 업그레이드	지원되는 운영 체제 버전으로 인스턴스를 업그레이드하여 인스턴스 마이그레이션을 방지합니다. 소프트웨어 공급업체의 자동화 및 업그레이드 기능을 활용하여 선택한 인스턴스에서 현재 위치 업그레이드를 수행할 수 있습니다(예: Microsoft Windows 2008 R2에서 Microsoft Windows 2012 R2로). 이 접근 방식은 새 인스턴스에 쉽게 다시 설치할 수 없는 레거시 애플리케이션에 이상적이며 이전 OS 버전에서 알려진 보안 위협과 완화되지 않은 보안 위협으로부터 추가 보호를 제공합니다. 현재 위치 업그레이드에는 다음 운영 체제가 지원됩니다. • Microsoft Windows 2012 R2에서 Microsoft Windows 2016 이상으로 • Microsoft Windows 2016에서 Microsoft Windows 2022 이상으로 • Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8로 • Red Hat Enterprise Linux 8에서 Red Hat Enterprise Linux 9로 • Oracle Linux 7에서 Oracle Linux 8로	이 솔루션은 새 인스턴스에 더 이상 다시 설치할 수 없는 애플리케이션(예: 소스 코드 손실, ISV 업무 중단 등)에 제공됩니다. 실패한 업그레이드를 원래 상태로 롤백할 수 있습니다. 운영 측면에서 롤백을 사용하는 것이 좋습니다. 최신 보안 패치를 사용하면 인스턴스가 더 지원 가능한 상태가 되기 때문입니다.

주제

- [온디맨드 AMS 작업 요청](#)
- [Operations on Demand 오퍼링 변경](#)

온디맨드 AMS 작업 요청

AWS Managed Services(AMS) OOD(Otions on Demand)는 AMS AWS 계정 에 온보딩된 모든에서 사용할 수 있습니다. Operations on Demand를 활용하려면 클라우드 서비스 제공 관리자(CSDM), 솔루션 아키텍트(SA), 계정 관리자 또는 클라우드 아키텍트(CA)에 추가 정보를 요청합니다. 사용 가능한 OOD 오퍼링은 이전 [오퍼링 테이블의 Operations on Demand 카탈로그](#)에 나열되어 있습니다. 참여 범위 조정이 완료되면 AMS Operations에 서비스 요청을 제출하여 OOD에 대한 참여를 시작합니다.

각 OOD 서비스 요청에는 참여와 관련된 다음과 같은 세부 정보가 포함되어야 합니다.

- 요청된 특정 OOD 제품 및 각 특정 OOD 제품:
 - 특정 OOD 상품에 할당할 블록 수(블록 1개는 해당 역월의 운영 리소스 시간 20시간과 동일하며, 해당 Operations on Demand 상품에 대해 AWS당시의 표준 요금으로 청구됨)입니다.
 - 특정 OOD 오퍼링이 요청되는 각 AWS Managed Services 계정의 계정 ID입니다.

OOD 서비스 요청은 다음 중 하나를 통해 제출해야 합니다.

- 해당 Operations on Demand 오퍼링을 수신하는 AWS Managed Services 계정 또는
- AWS Managed Services 계정인 멤버 계정을 대신하여 모든 기능 모드의 AWS Organizations 관리 계정인 AWS Managed Services 계정입니다.

OOD 서비스 요청이 수신되면 AMS Operations는 승인, 부분 승인 또는 거부로 계정을 검토하고 업데이트합니다.

OOD 오퍼링 서비스 요청이 승인되면 AMS와 사용자가 계약을 시작하도록 조정합니다. 서비스 요청이 승인되고 참여 시작 날짜가 합의될 때까지 OOD 오퍼링이 시작되지 않습니다.

AMS는 OOD 블록의 월별 구독 할당을 사용합니다. 새 서비스 요청을 통해 옵트아웃을 요청할 때까지 계약 시작 날짜부터 매월 승인된 블록 수를 할당합니다. OOD 블록은 한 달 동안 유효합니다. 미사용 블록 또는 블록 부분은 롤오버되거나 향후 달로 이월되지 않습니다.

실제로 사용한 시간에 관계없이 매월 최소 1개의 OOD 블록이 청구됩니다. 사용한 시간이 없는 추가 할당된 OOD 블록에는 요금이 청구되지 않습니다.

Operations on Demand 오퍼링 변경

OOD(Otions on Demand) 오퍼링에 대한 지속적인 참여 변경을 요청하려면 다음 정보가 포함된 서비스 요청을 제출합니다.

- 요청 중인 수정(들) 및
- 수정 사항이 적용되기 위해 요청된 날짜입니다.

OOD 서비스 요청을 수신한 후 AMS Operations는 요청을 검토하고 승인 또는 할당된 CSDM이 사용자와 협력하여 수정의 범위와 영향을 결정하는 요청으로 업데이트합니다. 수정으로 인해 CSDM의 범위 조정 작업이 필요한 것으로 확인되면 범위 조정 연습이 완료된 후 수정된 참여를 시작하기 위해 두 번째 OOD 서비스 요청을 제출해야 합니다.

승인되면 가장 최근에 수정된 블록 할당은 활성 상태가 되고 계속 활성 상태로 유지되며, AWS와 사용자가 달리 합의하지 않는 한 이전 블록 할당을 대체합니다.

문서 기록

다음 표에서는 AMS 고급 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

- API 버전: 2019-05-21
- 신규 또는 업데이트된 CTs 및 연습: [AMS 고급 변경 유형 참조 문서 기록](#).
- 새 AMS AMIs: [AMS Amazon Machine Image\(AMIs\)](#).

변경 사항	설명	날짜
AMS 고급 섹션의 표준 컨트롤에서 AWS Identity and Access Management (IAM)에 대한 표 업데이트	IAM 정책 및 Amazon S3 버킷에 대한 액세스와 관련하여 표의 정보가 업데이트되었습니다.	2025년 9월 25일
결제 관련 쿼리에 대한 단계를 업데이트했습니다.	AMS에서 서비스 요청 생성 섹션에서 결제 관련 쿼리에 대한 서비스 요청을 생성하는 단계가 업데이트되었습니다.	2025년 9월 25일
변경 유형에 대한 이메일 알림 정보 업데이트	RFC 이메일 알림 구성(콘솔) 섹션에서 변경 유형에 대한 이메일 알림을 추가하기 위한 정보와 예제를 업데이트했습니다.	2025년 9월 25일
업데이트된 변경 유형	AMS에서 생성한 리소스에 태그를 지정하기 위한 변경 유형으로 AMS 인프라 자동 태그 지정 섹션을 업데이트했습니다.	2025년 9월 25일
AWS Managed Services FAQ의 업데이트된 VM Import/Export	도구가 인스턴스에서 명령을 수행할 수 있도록 인스턴스 프로파일을 요청하는 데 사용되는 RFC를 업데이트했습니다.	2025년 9월 24일

[SUSE Linux Enterprise Server for SAP Applications 15 SP6 인스턴스 시작을 위한 변경 요청\(RFC\) 업데이트](#)

올바른 RFC를 사용하여 새로운 SAP 애플리케이션용 SUSE Linux Enterprise Server 15 SP6 인스턴스를 시작하는 방법에 대한 2단계가 업데이트되었습니다.

2025년 9월 22일

[변경 요청\(RFC\) 업데이트](#)

계정 AWS Elastic Disaster Recovery 내에 필요한 IAM 역할을 생성하기 위해 AWS Managed Services FAQ 섹션에서 올바른 RFC로 업데이트되었습니다.

2025년 9월 22일

[Trusted Remediator에서 지원하는 새로운 Trusted Advisor 비용 최적화 검사 4개 추가](#)

다음과 같은 비용 최적화 검사가 추가되었습니다.

2025년 9월 22일

- c1z7kmr00n - 인스턴스에 대한 Amazon EC2 비용 최적화 권장 사항
- c1z7kmr02n - 볼륨에 대한 Amazon EBS 비용 최적화 권장 사항
- c1z7kmr03n - DB 인스턴스에 대한 Amazon RDS 비용 최적화 권장 사항
- c1z7kmr05n - 함수에 대한 AWS Lambda 비용 최적화 권장 사항

[가용 영역\(AZs\)에 대한 참고 사항 업데이트](#)

AMS의 보안 그룹에 대한 정보가 업데이트되었습니다.

2025년 9월 5일

업데이트된 변경 유형

Managed AD를 애플리케이션 계정과 공유하도록 AWS Managed Services FAQ의 Amazon FSx 섹션을 변경 유형으로 업데이트했습니다.

2025년 9월 5일

업데이트된 변경 유형

삭제 API를 사용하도록 AWS Managed Services FAQ 섹션의 Amazon DocumentDB를 변경 유형으로 업데이트했습니다. APIs

2025년 9월 5일

업데이트된 변경 유형

Alexa for Business 게이트웨이를 설치 및 운영하기 위해 제한된 액세스 IAM 사용자 2명으로 변경 유형으로 AWS Managed Services FAQ의 Alexa for Business 섹션을 업데이트했습니다.

2025년 9월 5일

업데이트된 변경 유형

AWS Managed Services FAQ 섹션의 AppStream 2.0을 변경 유형으로 업데이트하여 모든 플릿 스트리밍 인스턴스에서 사용할 수 있는 IAM 역할을 생성하고 선택

2025년 9월 5일

업데이트된 변경 유형

EventBridge를 사용하여 다른 AWS 리소스를 트리거하기 전에 EventBridge 서비스 역할을 요청하도록 AWS Managed Services FAQ 섹션의 EventBridge를 변경 유형으로 업데이트했습니다.

2025년 9월 5일

Trusted Remediator의 업데이트된 Trusted Advisor 보안 검사 지원	Hs4Ma3G108 점검에 대해 지원되는 사전 구성된 파라미터 및 제약 조건 업데이트 - CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 함	2025년 9월 5일
Trusted Remediator의 업데이트된 Trusted Advisor 보안 검사 지원	Hs4Ma3G184 버전 2를 추가하도록 Trusted Advisor 보안 검사를 업데이트했습니다. Application Load Balancer 및 Classic Load Balancer 로깅을 활성화해야 합니다.	2025년 9월 5일
신뢰할 수 있는 수정자 섹션에서 지원하는 Trusted Advisor 운영 우수성 검사 업데이트	지원되는 새 검사 c1fd6b9614 Amazon S3 액세스 로그 활성화를 추가하도록 신뢰할 수 있는 수정자 섹션에서 지원하는 Trusted Advisor 운영 우수성 검사가 업데이트되었습니다.	2025년 8월 28일
업데이트된 변경 유형	사용자 지정 IAM 역할의 유형을 변경합니다.	2025년 8월 25일
AMS 섹션에서 .Net 및 SQL Server용 CloudWatch Application Insights 사용 업데이트	CloudWatch Application Insights를 사용하도록 변경 유형을 수정했습니다.	2025년 8월 25일
변경 요청(RFC) 업데이트	Amazon S3 버킷에 태그를 더 추가하기 위한 변경 요청(RFC).	2025년 8월 25일
변경 요청(RFC) 업데이트	관리 목적으로 AMS에서 생성한 모든 리소스에 태그를 지정하기 위한 변경 요청(RFC).	2025년 8월 25일

AWS Managed Services FAQ 섹션의 Lambda 업데이트	이벤트 소스를 생성하기 위해 다른 AWS 서비스에 액세스하기 위한 변경 유형을 수정했습니다.	2025년 8월 25일
AWS Managed Services FAQ 섹션의 Lambda 업데이트	Lambda 함수를 프로비저닝하도록 변경 유형을 수정했습니다.	2025년 8월 25일
보안 그룹 생성, 변경 또는 삭제 섹션 업데이트	스택 및 VPCs.	2025년 8월 25일
Compute Optimizer에 대한 새 콘텐츠를 포함하도록 신뢰할 수 있는 수정자 섹션 업데이트	지원되는 AWS Compute Optimizer 권장 사항에 대한 새 콘텐츠를 포함하도록 신뢰할 수 있는 수정자 섹션을 업데이트했습니다.	2025년 8월 18일
TOC 용어집 링크 제거됨	AWS 용어집 .	2025년 8월 8일
정확한 변경 유형 권장 사항	고객 지표를 애플리케이션 모니터링 시스템에 통합하려면 AMS에 배포 모니터링 및 알림 SNS CT 생성(ct-3dfnglm4ombbs)이 포함된 RFC를 제출하여 지표에 대한 Amazon SNS 주제 생성을 요청합니다.	2025년 8월 8일
정확한 변경 유형 권장 사항	자리 표시자 인스턴스 볼륨을 삭제하려면 관리 고급 스택 구성 요소 EBS 볼륨 변경 유형 삭제(ct-3e3h8u0sp5z80)를 제출합니다.	2025년 8월 8일
새로운 모니터링 알림: SecureChannelFailure 및 손상 된 보안 채널	AMS AMS의 기존 모니터링에 서 알림 자동 알림 수정 .	2025년 8월 8일

새로운 신뢰할 수 있는 수정자 검사

[Trusted Advisor Trusted Remediator Hs4Ma3G120-AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime, Hs4Ma3G230-AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 및 c18d2gz150-AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime](#)에서 지원하는 Trusted Remediator 보안 검사에서 지원하는 비용 최적화 검사입니다. [Trusted Advisor Hs4Ma3G120 AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime Hs4Ma3G230AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime](#)

2025년 8월 8일

포인트 3.2에서 IAM 표준 업데이트

언어를 명확히 하고 태그 지정에 대한 언급을 제거했습니다.

2025년 7월 25일

알림 옵트아웃 옵션 업데이트

태그를 추가하면 두 개의 알림을 추가로 옵트아웃할 수 있습니다.

2025년 7월 25일

셀프 서비스 프로비저닝 서비스 사용 중단

CloudEndure 셀프 서비스 프로비저닝 서비스는 더 이상 사용되지 않습니다 AWS Application Migration Service.

2025년 7월 25일

<u>백업을 위한 새로운 기능</u>	새 태그를 사용하여 백업 볼트에 대한 알림을 사용자 지정합니다.	2025년 7월 25일
<u>업데이트된 제어 테이블</u>	AMS-STD-002 - AWS Identity and Access Management (IAM) 테이블 섹션에서 일부 중복 제어를 제거했습니다.	2025년 6월 26일
<u>SSP 서비스 AWS Transfer Family 사전 조건 업데이트</u>	사전 조건 섹션에 정보가 추가되었습니다.	2025년 6월 26일
<u>업데이트된 IAM 정책 예제</u>	권장 사항에 따라 더 많은 제한 사항으로 IAM 정책 예제를 업데이트했습니다.	2025년 6월 26일
<u>AMI 지원 OSES 업데이트</u>	Ubuntu Linux 22.04에 Ubuntu Linux 24.04를 추가하고 모든 참조를 SP5에서 SP6으로 변경했습니다.	2025년 6월 26일
<u>셀프 서비스 프로비저닝 서비스, MediaStore 사용 중단</u>	에 대한 사용 중단 참고 사항이 추가되었습니다 AWS Elemental MediaStore.	2025년 6월 26일
<u>셀프 서비스 프로비저닝 서비스, Amazon Inspector Classic 사용 중단</u>	Amazon Inspector Classic에 대한 사용 중단 참고 사항이 추가되었습니다.	2025년 6월 26일
<u>셀프 서비스 프로비저닝 서비스, Amazon Connect 사용 중단</u>	Amazon Connect에 대한 사용 중단 참고 사항이 추가되었습니다.	2025년 6월 26일
<u>AMS에서 지원되는 구성에 대한 섹션 업데이트</u>	AMS에서 지원되는 운영 체제 및 지원되는 EOS(지원 종료) 운영 체제에 대해 지원되는 구성을 업데이트했습니다.	2025년 6월 25일

셀프 서비스 프로비저닝 서비스, WorkDocs 사용 중단	더 이상 사용되지 않는 WorkDocs에 대한 페이지 및 참조가 제거되었습니다.	2025년 6월 19일
대체 패치 리포지토리에 대한 패치 관리 중요 보안 참고 사항	AMS에서 대체 패치 리포지토리를 사용하기 위한 중요 보안 참고 사항 및 모범 사례입니다.	2025년 6월 10일
지원되는 운영 체제 업데이트	AMS Advanced 지원 운영 체제가 업데이트되고, 일부는 추가되고, 일부는 제거됩니다.	2025년 5월 22일
내부 전용 APIs	일부 CloudWatch 로그에 나타나는 내부 전용 APIs.	2025년 5월 22일
AMS 신뢰할 수 있는 수정자 업데이트	새 파라미터인 <code>preconfigured-parameters</code> 를 사용하여 신뢰할 수 있는 수정자에서 Trusted Advisor 검사를 사용자 지정하는 방법.	2025년 5월 22일
SSP Amazon Elastic Container Registry 업데이트	Amazon ECR 서비스를 온보딩하면 더 많은 역할이 자동으로 프로비저닝됩니다.	2025년 5월 8일
AMS Advanced Trusted Remediator FAQ 및 업데이트.	지원되는 Trusted Advisor 검사에 대한 몇 가지 업데이트, 신뢰할 수 있는 수정자 FAQ("신뢰할 수 있는 수정자는 계정에 어떤 리소스를 배포합니까?" 추가됨) 등이 있습니다. Trusted Advisor Trusted Remediator에서 지원하는 검사 도 참조하세요.	2025년 5월 8일
AMS 고급 표준 보안 제어 업데이트.	"보안 그룹 공유" 제어가 추가되었습니다.	2025년 5월 8일

AMS Advanced 보호 네임스페이스.	AMS 보호 네임스페이스 EPSMarketplaceSubscriptionRole 및가 EPS 추가되었습니다.	2025년 4월 24일
AMS Advanced 로그 위치.	추가 로그 위치가 추가되었습니다.	2025년 4월 24일
AppStream 2.0 사전 조건 업데이트를 위한 AMS 고급 셀프 서비스 프로비저닝 모드입니다.	AppStream 2.0의 사전 조건이 추가되었습니다. 서비스에 대한 프로비저닝 RFC를 제출할 때 Amazon S3 버킷 이름을 포함해야 합니다.	2025년 4월 24일
AMS Advanced New Amazon RDS 자동 수정 알림.	알림 ID:- 0224, 요청된 할당된 스토리지가 구성된 최대 스토리지 임계값에 도달하거나 초과할 때 트리거됩니다.	2025년 3월 27일
AMS Advanced AWS 는 2024년 7월 25일부터 Amazon CloudSearch에 대한 새로운 고객 액세스를 종료했습니다.	기존 고객은 여전히 서비스를 사용할 수 있지만 새로운 기능은 없습니다.	2025년 3월 27일
AMS Advanced AWS 는 2024년 7월 25 AWS CodeCommit 일부터에 대한 새로운 고객 액세스를 종료했습니다.	기존 고객은 여전히 서비스를 사용할 수 있지만 새로운 기능은 없습니다.	2025년 3월 27일
이제 신뢰할 수 있는 수정자를 사용할 수 있습니다.	이제 AWS Trusted Advisor 검사 문제 해결을 자동화하는 AWS Managed Services 솔루션인 Trusted Remediator를 사용할 수 있습니다.	2025년 3월 19일
AMS Advanced New 자동 수정 RDS 알림.	RDS-EVENT-0224가 추가되었습니다.	2025년 3월 17일

[AMS Advanced New 기능: 인시던트 알림.](#)

AppRegistry를 사용하여 애플리케이션을 생성하고 해당 애플리케이션에 대한 인시던트 알림을 사용자 지정할 수 있습니다.

2025년 3월 13일

[AMS RDS 경보 모니터링 임계값으로 업데이트.](#)

RDS 평균 CPU 사용률 경보 임계값이 75%에서 90%로 변경되었습니다.

2025년 2월 20일

[집계된 보고서 보기를 위한 새 데이터 옵션으로 셀프 서비스 보고서 업데이트](#)

다음 셀프 서비스 보고서에 Trusted AWS Organization account enabled by the customer 대한 새 필드 이름: Admin Account ID, 데이터 세트 필드 이름: aws_admin_account_id 및 정의:를 포함하도록 데이터 옵션을 추가했습니다.

2025년 1월 28일

- 패치 보고서(일별)
- 백업 보고서(일별)
- 인시던트 보고서(주별)

[AWS Batch SSP 업데이트](#)

다음 RFC를 사용하여 AMS 계정 AWS Batch 에서를 프로비저닝할 수 있습니다. 관리 | AWS 서비스 | 자체 프로비저닝된 서비스 | 추가(ct-1w8z66n899dct).

2025년 1월 28일

[새로운 AMS 기능: 집계된 셀프 서비스 보고서](#)

집계된 셀프 서비스 보고(SSR)를 사용하면 조직 수준, 교차 계정에서 집계된 기존 셀프 서비스 보고서를 볼 수 있습니다.

2025년 1월 21일

[Forecast SSP 섹션 업데이트](#)

참고: AWS 는 2024년 7월 29일부터 Amazon Forecast에 대한 새로운 고객 액세스를 종료했습니다. Amazon Forecast 기존 고객은 평소처럼 서비스를 계속 사용할 수 있습니다.

2025년 1월 10일

[AMS 보호 네임스페이스 섹션 업데이트](#)

AMS 보호 네임스페이스 목록에 누락된 보호 네임스페이스(*mc, *MC 및 *Mc)를 추가했습니다.

2025년 1월 9일

[모니터링 작동 방식 섹션 업데이트](#)

인시던트가 아닌 리소스 또는 인스턴스 ID별로 알림 알림을 구성하여 새 기능에 대한 정보를 추가했습니다.

2025년 1월 8일

[업데이트됨: 태그 기반 업데이트 콘텐츠](#)

키 이름의 오타를 수정하고 잘못된 구성 파일 경로를 수정했습니다.

2025년 1월 6일

[업데이트됨: AMS AMI 참고 사항](#)

Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.

2024년 11월 21일

[Operations On Demand 오퍼링 테이블 업데이트](#)

현재 위치 업그레이드에는 다 음 운영 체제가 지원됩니다.

2024년 11월 11일

- Microsoft Windows 2016에서 Microsoft Windows 2022 이상으로

Operations On Demand 오퍼링 테이블 업데이트

현재 위치 업그레이드에는 다음 운영 체제가 지원됩니다.

2024년 11월 1일

- Microsoft Windows 2012 R2에서 Microsoft Windows 2016 이상으로
- Red Hat Enterprise Linux 7에서 Red Hat Enterprise Linux 8로
- Red Hat Enterprise Linux 8에서 Red Hat Enterprise Linux 9로
- Oracle Linux 7에서 Oracle Linux 8로

지원되는 구성 업데이트

지원되는 Oracle Linux 운영 체제를 9.0-9.3, 8.0-8.9, 7.5-7.9로 업데이트했습니다.

2024년 10월 24일

업데이트된 AMS Amazon Machine Image(AMIs)

Windows 2012 및 2012 R2를 제거하도록 Windows 기반 AMIs를 업데이트했습니다. 더 이상 지원되지 않는 여러 AMIs를 제거하고 다음을 추가하도록 Linux 기반 AMIs를 업데이트했습니다.

2024년 10월 24일

- Amazon Linux 2(ARM64)
- RHEL 9
- SUSE Linux Enterprise Server 15 SP5

이제 태그 기반 알림에 여러 이메일 주소를 포함할 수 있습니다.

이제 태그 기반 알림에서 여러 이메일 주소가 지원됩니다.

2024년 9월 20일

변경 요청 보안 검토 섹션이 추가되었습니다.	변경 요청 보안 검토 프로세스에 대한 세부 정보를 제공하는 새 섹션이 추가되었습니다.	2024년 9월 17일
새 섹션이 추가되었습니다.	이제 AMS Advanced에서 변경 요청 보안 검토가 수행되는 방법을 설명하는 새 섹션을 사용할 수 있습니다.	2024년 9월 12일
AMS Advanced에서 지원하는 새로운 서비스입니다.	AWS Resilience Hub 는 이제 AMS Advanced에서 지원됩니다.	2024년 8월 30일
AMS Advanced에서 지원하는 새로운 서비스입니다.	이제 AMS Advanced에서 5가지 새로운 서비스를 지원합니다. • Amazon Bedrock • Amazon Kendra • Amazon Quantum Ledger Database(QLDB) • AWS Service Catalog AppRegistry • – Amazon Managed Service for Prometheus	2024년 8월 21일
이제 새 엔드포인트 보안 네트워크 기본 설정을 사용할 수 있습니다.	이제 업데이트 소스가 EPS 기본 네트워크 설정에 포함됩니다.	2024년 8월 21일
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	2024년 7월 30일
AMS는 이제 Amazon Route 53 Resolver DNS 방화벽을 지원합니다.	이제 AMS에서 Amazon Route 53 Resolver DNS 방화벽 지원합니다.	2024년 7월 30일

AWS DataSync SSPS 업데이트	AWS DataSync에는 더 이상 Amazon S3 버킷 이름에 "datasync-" 접두사가 필요하지 않습니다.	2024년 7월 30일
보안 구성 규칙 대시보드	이제 셀프 서비스 보고에서 보안 구성 규칙 대시보드를 사용할 수 있습니다.	2024년 7월 24일
AMS는 이제 Oracle Linux 8.9, RHEL 8.10 및 RHEL 9.4를 지원합니다.	AMS는 이제 Oracle Linux 8.9, RHEL 8.10 및 RHEL 9.4를 지원합니다.	2024년 7월 5일
이제 셀프 서비스 프로비저닝 모드에서 Amazon Bedrock 사용 가능	이제 AMS SSP 모드에서 Amazon Bedrock을 요청할 수 있습니다.	2024년 6월 27일
보안 인시던트 대응의 Amazon Route 53 Resolver DNS 방화벽 이벤트	이제 AMS가 보안 인시던트 대응에서 Amazon Route 53 Resolver DNS 방화벽 이벤트를 모니터링합니다.	2024년 6월 21일
AMS BYOEPS(Bring Your Own EPS) 기능을 활성화하는 방법에 대한 추가 정보가 추가되었습니다.	AMS BYOEPS(Bring Your Own EPS) 기능을 활성화하는 방법에 대한 추가 정보가 추가되었습니다.	2024년 6월 5일
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	2024년 5월 23일
셀프 서비스 프로비저닝 모드에서 사용자 지정 역할을 사용하는 AWS Amplify 방법에 대한 정보가 추가되었습니다(MALZ 환경만 해당).	MALZ 환경이 셀프 서비스 프로비저닝 모드에서 AWS Amplify와 함께 사용자 지정 역할을 사용하는 방법에 대한 지침이 추가되었습니다.	2024년 5월 23일

[이제 Amazon Kendra를 셀프 서비스 프로비저닝 모드에서 사용할 수 있습니다.](#)

이제 Amazon Kendra를 셀프 서비스 프로비저닝 모드에서 사용할 수 있습니다.

2024년 5월 23일

[AMS Advanced는 추가 운영 체제를 지원합니다.](#)

AMS Advanced는 Red Hat Enterprise Linux(RHEL) 9.x 및 Ubuntu 20.04 및 22.04를 지원합니다.

2024년 4월 25일

[AMS Advanced는 Amazon Linux 2용 ARM64 아키텍처를 지원합니다.](#)

AMS Advanced는 Amazon Linux 2용 ARM64 아키텍처를 지원합니다.

2024년 4월 25일

[다중 계정 랜딩 존\(MALZ\) 랜딩 존 계정 섹션에서 오프보드가 업데이트되었습니다.](#)

다중 계정 랜딩 존에서 애플리케이션 및 코어 계정을 오프보딩하는 방법에 대한 자세한 정보가 추가되었습니다.

2024년 4월 11일

[업데이트됨: 서비스 요청 관리 설명.](#)

서비스 설명 주제의 서비스 요청 관리 설명을 업데이트했습니다.

2024년 3월 21일

[업데이트됨: 인시던트 관리 서비스 약정 섹션.](#)

AMS 서비스 수준 계약에 대한 링크가 추가되었습니다.

2024년 3월 21일

[업데이트됨: 서비스 요청 관리 작동 방식 섹션.](#)

AMS가 기능 요청 또는 버그가 포함된 서비스 요청을 처리하는 방법에 대한 설명을 추가했습니다.

2024년 3월 21일

[업데이트됨: 지원 받기 섹션.](#)

새로운 결제 질문 섹션을 포함하도록 지원 받기 섹션을 업데이트했습니다.

2024년 3월 21일

[업데이트됨: AMS 자동 IAM 프로비저닝](#)

사용자 지정 거부 목록 정보로 AMS 자동 IAM 프로비저닝 업데이트

2024년 3월 21일

이전 업데이트

다음 표에서는 2024년 3월 이전의 AMS Advanced 가이드 설명서에 대한 중요한 변경 사항을 설명합니다.

변경 사항	설명	링크
2024년 2월		
지원되는 운영 체제 업데이트	SUSE Linux Enterprise Server 15 SP5를 포함하도록 지원되는 운영 체제를 업데이트했습니다.	지원되는 구성 섹션을 참조하세요
AMS의 기존 모니터링에서 알림에 대한 참고 사항이 추가되었습니다.	EC2 루트가 아닌 볼륨 사용에 대한 경보가 기본적으로 비활성화되어 있음을 나타내는 참고 사항이 추가되었습니다.	AMS의 기존 모니터링 알림 섹션을 참조하세요
모니터링 및 이벤트 관리에 새 섹션 AMS 이벤트 라우터를 추가했습니다.	AMS 고급 이벤트 라우터에 대해 설명하는 새 섹션이 추가되었습니다.	AMS에서 Amazon EventBridge 관리형 규칙 사용 섹션을 참조하세요
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.02.2024 참조
2024년 2월		
AMS Advanced의 Amazon EventBridge 규칙 서비스 연결 역할에 대한 새 섹션 추가	인프라 보안 섹션에 AMS Advanced의 Amazon EventBridge 규칙 서비스 연결 역할에 대한 새 섹션이 추가되었습니다.	AMS Advanced에 대한 Amazon EventBridge 규칙 서비스 연결 역할 참조
셀프 서비스 프로비저닝 모드 섹션 업데이트	셀프 서비스 프로비저닝 모드의 새 Amazon Inspector에	Amazon Inspector Classic(AMS SSPS) 참조

변경 사항	설명	링크
	대한 새 섹션이 추가되었습니다.	
2024년 1월		
계획된 이벤트 관리(PEM) 섹션 업데이트	계획된 이벤트 관리(PEM)에 추가 세부 정보와 FAW를 추가했습니다.	AWS Managed Services의 계획된 이벤트 관리 섹션을 참조하세요
SSM 에이전트 자동 설치에 대한 새 섹션 추가	자동 EC2 인스턴스 구성에서 SSM 에이전트 자동 설치에 대한 새 섹션이 추가되었습니다.	SSM 에이전트 자동 설치 섹션을 참조하세요
추가됨 AWS Resilience Hub (AMS SSPS)	새 SSPS 서비스가 추가되었습니다.	AMS SSP를 사용하여 AMS 계정 AWS Resilience Hub에서 프로비저닝 섹션을 참조하세요
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.01.2024 참조
2023년 12월		
AMS에서 직접 변경 모드 업데이트	새 하위 섹션인 직접 변경 모드 사용 사례를 AMS의 직접 변경 모드에 추가했습니다.	AMS의 직접 변경 모드 섹션을 참조하세요
업데이트됨 AWS Amplify (AMS SSPS)	Amplify를 요청하는 데 위험 수락이 필요함을 명확히 하기 위해 FAQ를 업데이트했습니다.	AMS SSP를 사용하여 AMS 계정 AWS Amplify에서 프로비저닝 섹션을 참조하세요
신규 AWS Elastic Disaster Recovery (AMS SSPS)	새 SSPS 서비스 추가	AMS SSP를 사용하여 AMS 계정 AWS Elastic Disaster Recovery에서 프로비저닝 섹션을 참조하세요

변경 사항	설명	링크
새로운 Amazon Managed Service for Prometheus(AMS SSPS)	새 SSPS 서비스 추가	AMS SSP를 사용하여 AMS 계정에서 Amazon Managed Service for Prometheus 프로비저닝 섹션을 참조하세요
연속성 관리 작동 방식 섹션을 업데이트했습니다.	새 하위 섹션인 AMS 백업 모니터링 및 보고를 추가했습니다.	연속성 관리 작동 방식 섹션을 참조하세요
새로운 Amazon DevOpsGuru(AMS SSPS)	새 SSPS 서비스 추가	AMS SSP를 사용하여 AMS 계정에서 Amazon DocumentDB(MongoDB 호환) 프로비저닝 섹션을 참조하세요
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.12.2023 을 참조하세요.
2023년 11월		
업데이트된 Amazon CloudWatch Synthetics(AMS SSPS)	올바른 역할 이름을 사용하도록 FAQs를 업데이트했습니다.	AMS SSP를 사용하여 AMS 계정에서 Amazon CloudWatch Synthetics 프로비저닝 섹션을 참조하세요
업데이트된 Amazon API Gateway 셀프 서비스 프로비저닝 모드	API Gateway 섹션에 추가 역할을 추가customer_apigateway_cloudwatch_role 했습니다.	AMS SSP를 사용하여 AMS 계정에서 Amazon API Gateway 프로비저닝 섹션을 참조하세요
셀프 서비스 프로비저닝 모드에 새 서비스 추가	AWS Service Catalog AppRegistry 셀프 서비스 프로비저닝 모드 섹션에 추가됨	AMS SSP를 사용하여 AMS 계정 AWS Service Catalog AppRegistry 에서 프로비저닝 섹션을 참조하세요

변경 사항	설명	링크
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes .11.2023 을 참조하세요.
2023년 9월		
패치 오케스트레이터 사용에 대한 참고 사항 추가	패치 오케스트레이터 사용 섹션에 다음 참고 사항이 추가되었습니다. “운영 체제가 지원되지 않거나 유지 관리 기간 동안 중지된 인스턴스에 대해서는 패치 실패 알림이 생성되지 않습니다.”	AMS의 패치 관리 섹션을 참조하세요
추가 서비스로 데이터 암호화 업데이트	AMS의 데이터 암호화에 서비스가 추가되었습니다.	AMS의 데이터 보호 섹션을 참조하세요
RFC 오류 메시지에 새 단락을 추가했습니다.	서비스 요청 생성 링크를 추가하는 새 단락이 추가되었습니다.	AMS의 RFC 오류 문제 해결 섹션을 참조하세요
IAM 역할 이름을 수정했습니다.	IAM 역할 이름 customer_emr_cluster_autoscaling_role을 수정했습니다.	AMS의 셀프 서비스 프로비저닝 모드 섹션을 참조하세요
기본 모니터링 정보 업데이트	더 이상 사용되지 않는 두 경보 RDSReadLatencyAlarm 및 RDSWriteLatencyAlarm에 대한 참조를 제거했습니다.	AMS의 기본 모니터링 알림 섹션을 참조하세요
2023년 8월		
추가됨: AMS 보안 인시던트 대응	AMS 보안 인시던트 대응 사용에 대한 설명서가 추가되었습니다.	AMS의 보안 인시던트 대응 섹션을 참조하세요

변경 사항	설명	링크
2023년 7월		
추가됨: 자동 IAM 프로비저닝	자동 IAM 프로비저닝 사용에 대한 설명서가 추가되었습니다.	자동 IAM 프로비저닝 AMS 섹션을 참조하세요
업데이트됨: 액세스 역할 테이블	AMS Access에 누락된 역할이 추가되었습니다.	AMS 고객 계정 액세스 IAM 역할 섹션을 참조하세요
2023년 6월		
업데이트됨: 모니터링되는 RDS 알림 목록입니다.	AMS 기준 모니터링을 위한 RDS 알림 목록을 업데이트했습니다. 새로운 RDS 알림 유형 9개가 추가되었고 기존 RDS 알림 유형 3개가 제거되었습니다.	AMS의 기준 모니터링 알림 을(를) 참조하세요.
업데이트됨: 액세스 역할 테이블	AMS 보안에 대한 새 역할입니다.	AMS 고객 계정 액세스 IAM 역할 섹션을 참조하세요
2023년 5월		
업데이트됨: 서비스 결제 시작일 정책.	결제 시작일에 대한 정의가 업데이트되었습니다.	AMS 키 용어 을(를) 참조하세요.
2023년 4월		
업데이트됨: 월별 결제 셀프 서비스 보고서.	참고 추가: 월별 결제 보고서는 Management Payer 계정(AMS Advanced 다중 계정 랜딩 존)에서만 사용할 수 있지만 연결된 모든 AMS Accelerate 관리형 계정에 사용할 수 있습니다.	결제 보고서(월별) 을(를) 참조하세요.
업데이트됨: "Standard Patching" 콘텐츠 제거	AMS는 패치 오케스트레이터를 사용합니다.	AMS의 패치 관리

변경 사항	설명	링크
업데이트됨: AMS란 무엇입니까?	이전에 AMS란 무엇입니까?에서 일부 주제를 AMS 서비스 설명의 일부로 이동했습니다.	서비스 설명
업데이트됨: 다중 계정 랜딩 존 오프보딩	다양한 설명을 작성했습니다.	AMS 다중 계정 랜딩 존 계정에서 오프보딩
업데이트됨: AWS Transfer Family(AMS SSPS)	전송 설정 자습서에 대한 링크가 추가되었습니다.	AMS SSP를 사용하여 AMS 계정 AWS Transfer Family에서 프로비저닝
업데이트된 콘텐츠: 셀프 서비스 프로비저닝	AWS 법률에서 "CodeSuite"를 "Code services"로 대체했습니다.	AMS SSP를 사용하여 AMS 계정에서 AMS 코드 서비스 프로비저닝
업데이트된 콘텐츠: CloudWatch 지표 및 경보	예: 용어 발생 횟수에 대한 링크가 추가되었습니다.	AMS에서 사용자 지정 CloudWatch 지표 및 경보 생성
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.04.2023
2023년 3월		
업데이트된 콘텐츠: AMS에서 오프보딩	다중 계정 랜딩 존 계정을 오프보딩할 때 삭제되는 리소스를 명확히 함	AMS 다중 계정 랜딩 존 계정에서 오프보딩
업데이트됨: AMS AMIs	문서 기록 섹션에 매월 AMI ZIP 파일에 대한 링크가 추가되었습니다.	문서 기록
업데이트됨: 자동 문제 해결	EC2 볼륨 자동화에 대한 LVM 지원이 제거되었습니다.	알림의 AMS 자동 문제 해결

변경 사항	설명	링크
업데이트됨: 패치 RACI	패치 적용을 위한 RACI에 대한 몇 가지 업데이트 및 설명입니다.	AMS 책임 매트릭스(RACI)
업데이트된 콘텐츠: 셀프 서비스 프로비저닝	FAQ 글머리 기호가 추가되었습니다. 새 AWS Datasync 에이전트를 시작하려면 WIGS 수집이 필요하지 않습니다.	AMS의 셀프 서비스 프로비저닝 모드
업데이트된 콘텐츠: 셀프 서비스 프로비저닝	FAQ 글머리 기호가 추가되었습니다. 새 AWS Datasync 에이전트를 시작하려면 WIGS 수집이 필요하지 않습니다.	AMS의 셀프 서비스 프로비저닝 모드
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.03.2023
2023년 2월		
업데이트된 콘텐츠: AMS에서 오프보딩	다중 계정 랜딩 존 환경, VPCs 및 애플리케이션 계정을 오프보딩하는 방법을 명확히 함	AMS 계정 오프보드
업데이트된 콘텐츠: ARNs 찾기	DynamoDB 테이블 ARN을 찾기 위한 DynamoDB describe-table CLI 추가	AMS에서 Amazon 리소스 이름(ARNs) 찾기

변경 사항	설명	링크
업데이트된 콘텐츠: 셀프 서비스 프로비저닝	실제 SSPS가 아니므로 AMS "CodeSuite" 옵션을 제거했습니다. 관리 AWS 서비스 자체 프로비저닝 서비스 추가(검토 필요)(ct-3qe6io8t6jtny) 변경 유형을 계속 사용하고 CodeBuild, CodeDeploy 및 CodePipeline의 세 가지 서비스를 요청할 수 있습니다. 그런 다음 AMS는 계정에 customer_codebuild_service_role , customer_codedeploy_service_role 및 IAM 역할을 프로비저닝합니다aws_code_pipeline_service_role . 계정에 프로비저닝한 후에는 페더레이션 솔루션의 역할을 온보딩해야 합니다.	AMS의 셀프 서비스 프로비저닝 모드
업데이트된 콘텐츠: Secrets Manager 업데이트	다중 계정 랜딩 존(MALZ)과 단일 계정 랜딩 존(SALZ)에 필요한 역할을 수정했습니다.	Secrets Manager FAQ를 사용하여 키 공유
업데이트된 콘텐츠: 알림의 AMS 자동 수정	논리적 볼륨 관리자(LVM) 볼륨에 대한 지원이 추가되었습니다.	EC2 볼륨 사용량 수정 자동화
업데이트된 콘텐츠: AMS Amazon Machine Image(AMIs)	계정에서 AMIs를 제거하기 위해 샘플 코드를 사용하여 AMS AMIs 오프보딩 섹션을 추가했습니다.	AMS Amazon Machine Image(AMIs)

변경 사항	설명	링크
업데이트된 콘텐츠: IAM 사용자 역할	IAM 정책 업데이트: AMSBillingPolicy.	AMS의 IAM 사용자 역할
새 콘텐츠: 지원되지 않는 OSes	AMS가 지원되지 않는 운영 체제(OSes)에 제공하는 서비스에 대한 정보가 추가되었습니다.	AMS에서 지원되지 않는 운영 체제의 기능
업데이트된 콘텐츠: 온디맨드 보고서	특정 온디맨드 보고서는 AMS Advanced에서 사용할 수 없으며 사용 가능한 것으로 잘못 표시되었습니다.	요청 시 보고서
업데이트된 콘텐츠: AMS 계정 오프보딩	MALZ 애플리케이션 계정 오프보딩 지침을 명확히 했습니다.	AMS 애플리케이션 계정 오프보딩
업데이트된 콘텐츠: Secrets Manager	Secrets Manager를 사용하는데 필요한 IAM 역할의 이름을 수정했습니다.	AWS Managed Services FAQ의 Secrets Manager
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.02.2023
2023년 1월		
새 콘텐츠: AWS Device Farm(AMS SSPS)	새 SSPS 서비스: AWS Device Farm이 추가되었습니다.	AMS SSP를 사용하여 AMS 계정 AWS Device Farm에서 프로비저닝
업데이트됨: 지원되는 Windows 버전	Windows Server 2022에 대한 지원이 추가되었습니다.	AMS Amazon Machine Image(AMIs), 지원되는 구성 및 SNS를 사용한 AMS AMI 알림
업데이트됨: 연속성 관리	기본 AMS 백업 계획의 규칙을 업데이트했습니다.	기본 백업 계획, 다중 계정 랜딩 존

변경 사항	설명	링크
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.01.2023
2022년 12월		
업데이트됨: Bastions 사용	잘못된 링크를 수정했습니다.	Bastion을 사용하여 인스턴스에 액세스
업데이트됨: Resource Scheduler	몇 가지 개선 사항을 적용하고 더 많은 컨텍스트를 위해 AWS 인스턴스 스케줄러에 대한 링크를 추가했습니다.	AWS Managed Services 리소스 스케줄러
업데이트됨: Windows AMIs 및 지원되는 구성(새 Windows AMIs 경우)	EC2Launch(Windows Server 2016 이상)에서 EC2Launch (Windows Server 2016 및 Windows Server 2019)로 추가된 AMS AMI 콘텐츠를 업데이트하고 EC2LaunchV2(Windows Server 2022 이상)를 추가했습니다. Windows 기반 AMIs Microsoft Windows Server(2012, 2012 R2, 2016 및 2019)에서 Microsoft Windows Server(2012, 2012 R2, 2016, 2019 및 2022)로 업데이트했습니다.	AMS Amazon Machine Image(AMIs) 및 서비스 설명
업데이트됨: Resourced Scheduler 섹션	AMS Resource Scheduler를 배포하고 사용자 지정하는 방법을 개선했습니다.	AWS Managed Services 리소스 스케줄러
업데이트됨: AMS 설정: 프라이빗 및 퍼블릭 DNS	DNS 아키텍처 다이어그램을 업데이트했습니다.	프라이빗 및 퍼블릭 DNS 설정

변경 사항	설명	링크
업데이트됨: MALZ 네트워크 아키텍처	다이어그램을 업데이트하고 애플리케이션 계정 가속화에 대한 지침을 추가했습니다.	MALZ 네트워크 아키텍처
업데이트됨: 설정: 태그 사용	새 참고 사항: 사용자 지정 태그 지정은 코어 계정이 아닌 MALZ 애플리케이션 계정에서만 지원됩니다.	AMS 인프라 자동 태그 지정
업데이트됨: 액세스 관리: Bastion 사용	RDP 접속을 포함하도록 소개를 업데이트했습니다.	단일 계정 랜딩 존(SALZ) 접속 비용 절감
업데이트됨: AMS 기본 설정: 알림	EC2 인스턴스: 알림 테이블에 루트가 아닌 볼륨 사용량이 추가되었습니다.	AMS의 기본 모니터링 알림
업데이트됨: 연속성 관리	연속 백업에 대한 지침이 추가되었습니다.	연속성 관리 작동 방식
업데이트됨: 자동 EC2 인스턴스 구성	PowerBroker Identity Service(PBIS) 및 온 인스턴스 코드(OIC)에 대한 지원이 추가되었습니다.	Linux 인스턴스에서 PBIS 자동 업데이트 및 Linux 인스턴스에서 코드 자동 업데이트
업데이트됨: Secrets Manager에 대한 셀프 서비스 프로비저닝	계정에 Secrets Manager를 추가하기 위한 CT를 업데이트 FAQs 아래).	AMS SSP를 사용하여 AMS 계정 AWS Secrets Manager에서 프로비저닝
업데이트됨: 로그 관리	EC2 시스템 수준 로그 목록을 업데이트했습니다.	Amazon Elastic Compute Cloud(Amazon EC2) - 시스템 수준 로그
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.12.2022

변경 사항	설명	링크
2022년 11월		
업데이트됨: AMS Amazon Machine Image(AMIs)	지원되는 SUSE Linux 버전을 업데이트했습니다.	AMS Amazon Machine Image(AMIs)
업데이트됨: MALZ 계정	고객 관리형 애플리케이션 계정 삭제에 대한 지침이 추가되었습니다.	고객 관리형 애플리케이션 계정
업데이트됨: AMS 설정	customer-ams-amazon2-security-enhanced 추가.	SNS를 사용한 AMS AMI 알림
업데이트됨: 모니터링 작동 방식	서비스 알림 및 인시던트 보고서에 대한 설명을 업데이트했습니다.	모니터링 작동 방식
업데이트됨: MALZ 애플리케이션 계정 유형	계정 유형에 대한 설명을 개선했습니다.	애플리케이션 계정 유형
업데이트됨: 개발자 모드	개발자 모드에 대한 경고가 추가되었습니다.	AMS 개발자 모드를 시작하기 전에
업데이트됨: 계획된 이벤트 관리	섹션 추가: PEM 유형	AWS Managed Services의 계획된 이벤트 관리
업데이트됨: Amazon Machine Image(AMIs)	지원되는 SUSE Linux 버전 업데이트	AMS Amazon Machine Image(AMIs)
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.11.2022
2022년 10월		

변경 사항	설명	링크
신규: 자동 인스턴스 구성	새 섹션에서는 자동 인스턴스 구성 프로세스에 대해 설명합니다.	AMS Advanced의 자동 인스턴스 구성
신규: 일부 SSPS에는 수동 CT만 허용됩니다.	SSPS 추가를 위한 자동 CT가 아닌 수동 CT를 사용하도록 50개 이상의 셀프 서비스 프로비저닝 서비스 FAQs가 업데이트되었습니다.	AMS의 셀프 서비스 프로비저닝 모드
업데이트: AMS 설정	MALZ용 Amazon EC2 IAM 인스턴스 프로파일에 두 가지 정책이 추가되었습니다.	EC2 IAM 인스턴스 프로파일
신규: 사용자 지정 탐지 및 예방 규칙 라이브러리.	여러 고객의 학습을 기반으로 한 서비스 제어 정책(SCPs) 및 예방 Config 규칙 제어 예제 세트를 추가했습니다.	큐레이션 SCPs 및 구성 규칙
업데이트:경 AWS Backup 고	"변경 사항이 손실될 수 있으므로 AMS 백업 계획을 편집하지 마세요. 대신 사용자 지정 구성에 ct-2hyozbpa0sx0m을 사용하여 새 백업 계획을 생성합니다."	연속성 관리 작동 방식
Update: AWS Backup caution	페더레이션에 새 IAM 역할을 추가하는 방법에 대한 참고 사항이 추가되었습니다.	AMS Advanced에 IAM 리소스 배포
업데이트: 관리 모니터링	알림은 서비스 요청이 아닌 인시던트 보고서를 생성합니다.	모니터링 작동 방식
업데이트: 자체 EPS 가져오기	SALZ 및 MALZ에 적용됩니다.	AMS에서 자체 EPS 사용
업데이트: 애플리케이션 계정 가속화	Accelerate 계정이 애플리케이션 계정임을 명확히 했습니다.	애플리케이션 계정 유형

변경 사항	설명	링크
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.10.2022
2022년 9월		
업데이트됨: 리소스를 찾기 위한 CLI 명령 예제	--region 옵션이 필요할 수 있다는 새로운 예외를 추가했습니다.	필요한 데이터 찾기(SKMS), AMS
업데이트됨: IAM 역할 프로비저닝	이제 사용하여 IAM 역할을 생성하고 관리할 수 있습니다AWSManagedServices CloudFormationAdminRole .	Direct Change 모드를 사용하여 스택 생성
업데이트됨: AMS 기술 표준	AMS-STD-007 로깅: (#20) 전달 요구 사항을 명확히 했습니다.	보안 및 규정 준수
업데이트됨: 연속성 관리 작동 방식	백업 작업 시작 문구를 "기존"이 아닌 "온디맨드"로 수정했습니다.	연속성 관리 작동 방식
업데이트됨: 보안 및 규정 준수	표준 AMS-STD-007 번호 20: 계정 간 로그 전달에 대한 설명 및 지침이 업데이트되었습니다.	보안 및 규정 준수
업데이트됨: 변경 관리 사용 사례	레거시 변경 관리 사용 설명서에 대한 끊어진 링크를 제거했습니다.	변경 관리 사용 사례
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.09.2022

변경 사항	설명	링크
2022년 8월 11일		
업데이트됨: 일관성 및 가독성을 위한 장 제목, 일부 주제 하위 섹션을 더 적절한 섹션으로 이동	이제 "MALZ 네트워크 아키텍처"와 "SALZ 네트워크 아키텍처"가 모두 최상위 "네트워크 아키텍처" 섹션의 하위 섹션인 이전 "AMS 네트워크 아키텍처" 섹션입니다. "변경 관리를 위한 모드"는 "변경 관리"의 새로운 제목입니다. "기본 설정"은 이제 "AMS 설정"의 하위 섹션입니다. "AD FS 클레임 규칙 및 SAML 설정"(이전의 "ActiveDirectory Federation Services(ADFS) 클레임 규칙 및 SAML 설정)은 이제 "AMS 설정"의 하위 섹션입니다. "액세스 관리"는 "AMS에서의 액세스"에 대한 새로운 제목이며 TOC에서 이동합니다. "필요한 데이터 찾기"는 "서비스 지식 관리"의 새로운 제목입니다. "보고서 및 옵션"은 "AMS 보고"의 새로운 제목이며 TOC에서 더 낮습니다. 이제 "주문형 작업"이 TOC의 마지막 주제입니다.	AWS Managed Services란 무엇입니까?

변경 사항	설명	링크
업데이트됨: 결과 및 ARN, 신규: ARN을 사용하여 리소스 찾기	두 절차 모두 유용성을 위해 완전히 다시 작성되었습니다.	AMS에서 Amazon 리소스 이름 (ARNs) 찾기 및 AMS에서 ARN으로 리소스 찾기 .
업데이트됨: Transit Gateway에 CMA 연결	자동화는 코어 라우팅 도메인에 경로 추가를 지원하지 않으며 프로시저를 업데이트해야 합니다.	Transit Gateway에 CMA 연결
업데이트됨: MALZ 기본 구성 요소 요금	모든 가격은 달러 기호 형식의 미국 달러입니다.	AMS 환경 기본 구성 요소
업데이트됨: AMS AMI 참고 사항	Zip 파일에는 최신 AMS Amazon 머신 이미지(AMIs)에 대한 메모와 최신 AMIs.	AMIs.csv-and-notes.08.2022
2022년 7월 14일		
업데이트됨: 셀프 서비스 보고	KMS 키로 AWS Glue 메타데이터를 암호화하기 위한 지침이 추가되었습니다.	셀프 서비스 보고서
업데이트됨: AMS 기준 모니터링	DeleteRecoveryPoint 백업 알림이 추가되었습니다.	AMS의 기준 모니터링 알림
업데이트됨: 지원되는 운영 체제	Amazon Linux 2에 대한 지원 종료 날짜가 추가되었습니다.	지원되는 구성
업데이트됨: 셀프 서비스 프로비저닝	AWS Transfer SSPS에 대한 사전 조건을 추가했습니다.	AMS SSP를 사용하여 AMS 계정 AWS Transfer Family에서 프로비저닝
업데이트됨: AMS 보고	옵트인 리전에 대한 참고 사항이 추가되었습니다.	보고서 및 옵션

변경 사항	설명	링크
업데이트됨: RFC 서신 및 첨부 파일	허용되는 텍스트 파일 유형을 명확히 했습니다. 특히 YAML 파일은 .yaml(.yml 아님)로 끝나야 합니다.	RFC 서신 및 첨부 파일 추가 (콘솔)
2022년 6월 21일		
업데이트된 콘텐츠	이전에는 "변경 관리 모드" 또는 "표준 CM 모드"라고 했던 AMS 모드를 이제 "RFC 모드"라고 합니다. 모드 섹션이 확장되었습니다.	모드 개요.
새 경고	AWS Backup 경보를 추가했습니다.	AMS의 기존 모니터링 알림
2022년 6월 16일		
새로운 내용	인시던트 관리. 보안 위협이 아닌 인시던트는 이제 인시던트 보고서에서 사용자의 승인을 받아 AMS에서 해결할 수 있으며 별도의 RFC 및 승인이 필요하지 않습니다.	인시던트 관리
업데이트된 콘텐츠	MALZ: 네트워크 아키텍처 다이어그램을 업데이트했습니다. 업데이트: 마스터 계정 VPC에서 공유 서비스 vpc로의 VPC 피어링은 존재하지 않으므로 제거해야 합니다.	네트워킹 계정 아키텍처

변경 사항	설명	링크
	Sagemaker 셀프 서비스 프로비저닝 서비스(SSPS). Sagemaker의 사용을 위해 온보딩 시 추가된 새 IAM 역할로 업데이트되었습니다.	AMS SSP를 사용하여 AMS 계정에서 Amazon SageMaker AI 프로비저닝
	SNS 알림에 지원되는 AMIs 목록: customer-ams-sles12, customer-ams-sles15, customer-ams-amazon1-security-enhanced, customer-ams-rhel8, customer-ams-rhel8-security-enhanced, customer-ams-ubuntu18, customer-ams-windows2012, customer-ams-windows2019, customer-ams-windows2019-security-enhanced. customer-ams-rhel6 및 customer-ams-rhel6-security-enhanced AMIs.	SNS를 사용한 AMS AMI 알림
	에스컬레이션 이메일을 제거했습니다.	AWS Managed Services에 대한 도움말 보기
	주제 목록을 아래 열린 단락으로 이동했습니다.	AWS Managed Services란 무엇입니까?
	로드 밸런싱 로그에 대한 더 나은 링크로 서비스 로그를 업데이트하고 형식을 다시 지정했습니다.	AMS 집계 서비스 로그

변경 사항	설명	링크
EKS 셀프 서비스 프로비저닝 서비스(SSPS). 클러스터에서 봉투 보안 암호 암호화를 활성화하는 방법에 대한 정보가 추가되었습니다.	AMS SSP를 사용하여 AMS 계정 AWS Fargate 의에서 Amazon EKS 프로비저닝	
2022년 6월 9일		
업데이트된 콘텐츠, 도움 받기	에스컬레이션 경로 이메일을 제거했습니다. AMS는 인시던트 보고서, 서비스 요청 및 RFCs 통해 통신 방법을 제공합니다.	AWS Managed Services에 대한 도움말 보기
2022년 5월 12일		
새로운 콘텐츠, OOD(Options on Demand) 구독 모델	AMS는 현재 가입 및 갱신 모델에서 구독 할당 및 기본 옵트인 모델로 Operations on Demand 온보딩을 변경했습니다. AMS 계정을 온보딩하면 지금 Operations on Demand에 자동으로 등록됩니다.	온디맨드 작업
2022년 4월 14일		
새 콘텐츠, 비용 최적화	AMS는 비용 최적화를 위한 권장 사항을 제공합니다.	AWS Managed Services의 비용 최적화
업데이트된 콘텐츠, MALZ의 Accelerate 계정	잘못된 역할 이름(CustomerDefaultAdminRole)이 올바른 역할 이름(AccelerateDefaultAdminRole)으로 업데이트되었습니다.	AMS Accelerate 계정 "엑셀러레이트 계정 액세스" 섹션.

변경 사항	설명	링크
업데이트된 콘텐츠, AMS 액세스 IAM 역할	계정에 액세스하는 데 사용되는 다른 AMS IAM 역할이 추가되었습니다.	AMS가 계정에 액세스하는 이유와 시간 "AMS 고객 계정 액세스 IAM 역할" 섹션.
업데이트된 콘텐츠, AMS 백업 계획	AMS 관리형 백업 계획이 추가되었습니다.	AMS 백업 계획 및 AMS 백업 볼트
업데이트된 콘텐츠, AWS Secrets Manager	FAQ를 업데이트했습니다.	AMS SSP를 사용하여 AMS 계정 AWS Secrets Manager에서 프로비저닝
업데이트된 콘텐츠, DCM(Direct Change Mode) 온보딩	AMS는 Service Catalog 고객을 DCM에 온보딩하는 기능을 지원하지 않습니다.	직접 변경 모드 시작하기
업데이트된 콘텐츠, 서비스 설명	지원되는 서비스 섹션을 명확히 했습니다. • AWS Fargate의 Amazon EKS -> Fargate의 Amazon Elastic Kubernetes Service • Fargate용 Amazon ECS -> AWS Fargate의 Amazon Elastic Container Service • Amazon Kinesis -> Amazon Kinesis Data Streams	지원되는 AWS 서비스
업데이트된 콘텐츠, MALZ 계정 오프보딩	오프보딩 애플리케이션 계정에 대한 새로운 변경 유형을 참조하도록 업데이트되었습니다.	AMS 애플리케이션 계정 오프보딩

변경 사항	설명	링크
업데이트된 콘텐츠, 개발자 모드 인시던트 관리	인시던트 SLA 설명을 로 업데이트했습니다. AMS SLA는 AMS 변경 관리(개발자 모드 포함) 외부에서 생성되거나 업데이트된 리소스에는 적용되지 않으므로 개발자 모드에서 업데이트되거나 생성된 리소스는 자동으로 P3로 성능이 저하되며 지원이 최선의 노력입니다.	AMS 개발자 모드에서의 인시던트 관리
업데이트된 콘텐츠, DCM 온보딩	이제 새 DCM에 대한 RFC 템플릿에 SAML 공급자 ARN에 대한 필드가 포함됩니다.	직접 변경 모드 시작하기
업데이트된 콘텐츠, 용 DCM AWS CloudFormation	이제 AWS CloudFormation 스택 생성 및 업데이트 지침에 YAML 예제가 포함되어 있습니다.	AMS 변환
업데이트된 콘텐츠, MALZ 도구 계정	마이그레이션을 위한 새 IAM 역할이 있습니다AWSManagedServicesMigration Role .	AWS Application Migration Service(AWS MGN) 및 새 AMS 도구 계정에 대한 액세스 활성화
새로운 콘텐츠, 다중 계정 랜딩 존 계정	다중 계정 랜딩 존 AMS 관리 계정에서 Accelerate 계정을 생성할 수 있습니다.	AMS Accelerate 계정
업데이트된 콘텐츠, API/CLI SDK 설치	설치 지침에 Mac/Linux 설치에 대한 잘못된 파일 이름과 잘못된 명령이 나열되었습니다. 이 문제는 수정되었습니다.	AMS API 및 CLI 사용

변경 사항	설명	링크
업데이트된 콘텐츠, MALZ의 Accelerate 계정	잘못된 규칙 이름(CustomerDefaultAdminRole)이 있으며 올바른 규칙 이름(AccelerateDefaultAdminRole)으로 업데이트되었습니다.	AMS Accelerate 계정, "엑셀러레이트 계정 액세스" 섹션
업데이트된 콘텐츠, 모니터링	루트 사용량 모니터링이 85%에서 95%로 수정되었습니다.	AMS의 기존 모니터링 알림
업데이트된 콘텐츠, AMI 알림	새 AMS AMIs, 다양한 유형 생성에 대한 정보가 추가되었습니다.	SNS를 사용한 AMS AMI 알림
업데이트된 콘텐츠, AMS 기본 설정	Macie Classic에 대한 참조를 제거하고 Macie로 대체했습니다.	AMS의 기존 모니터링 알림
업데이트된 콘텐츠, AMS 예약 접두사	예약된 접두사 목록을 영문자로 묶었습니다.	AMS 예약 접두사
업데이트된 콘텐츠, 서비스 설명	변경 관리 및 셀프 서비스 프로비저닝에 대한 기능 섹션이 AMS 모드에 대한 자세한 정보로 업데이트되었습니다.	AWS Managed Services(AMS) AMS Advanced 운영 계획 기능
업데이트된 콘텐츠, AWS Secrets Manager	Secrets Manager를 사용하여 키 공유.	2022년 2월 10일
새 콘텐츠, 셀프 서비스 프로비저닝, Amazon Connect	아웃바운드 또는 인바운드 통화의 국가 목록을 추가하도록 요청하는 방법에 대한 FAQ가 추가되었습니다.	2022년 2월 10일

변경 사항	설명	링크
새로운 콘텐츠, 셀프 서비스 프로비저닝, Fargate의 Amazon EKS	AWS 클라우드 개발 키트 (CDK) 또는 CloudFormation Ingest를 통해 EKS 클러스터를 배포하는 것은 AMS에서 지원되지 않는다는 FAQ 제한이 추가되었습니다.	2022년 2월 10일
변경된 콘텐츠, 개발자 모드	수정했습니다. RFC 또는 서비스 요청을 사용하여 페더레이션 솔루션에 사용자를 할당하지 않고 솔루션에 따라 직접 할당합니다.	2022년 2월 10일
콘텐츠 변경, Direct Change 모드(DCM)	IAM은 DCM에서 지원되지 않습니다.	2022년 2월 10일
	DCM, 수행하는 검증을 기록해 둡니다.	2022년 2월 10일
	DCM, 다양한 역할의 제한을 명확히 합니다.	2022년 2월 10일
콘텐츠 변경, 기준 알림 모니터링	Redshift 클러스터 리소스 알림이 변경되었습니다.	2022년 2월 10일
콘텐츠 변경, 셀프 서비스 보고	고객이 보고서를 가져오는 데 사용할 정확한 s3 버킷 이름 (ams-reporting-data-account_ID)을 추가했습니다.	2022년 2월 10일

변경 사항	설명	링크
콘텐츠 변경, 수동 관리 대신 자동 변경 유형을 참조하도록 콘텐츠 업데이트 기타 기타 (MOO)	자동 변경 유형을 참조하도록 다중 계정 랜딩 존(MALZ) 애플리케이션 계정 콘텐츠를 업데이트했습니다(3개, "TGW 연결을 라우팅 테이블에 연결", "TGW 라우팅 테이블에서 경로를 생성하여이 VPC에 연결", "AMS 다중 계정 랜딩 존 전송 게이트웨이를 가리키도록 VPC 라우팅 테이블 구성"). AMS에서 생성된 알림 수신 태그 기반 알림	2022년 2월 10일
콘텐츠 변경: AMS AMIs	보안 강화 AMIs 대한 새로운 정보가 추가되었습니다. 지원되는 구성, AMS Amazon Machine Image(AMIs) 및 단원을 참조하십시오 보안 강화 AMIs.	2022년 1월 27일
새 콘텐츠: 셀프 서비스 프로비저닝.	Amazon Fsx for OpenZFS가 추가되었습니다. AMS SSP를 사용하여 AMS 계정에서 Amazon FSx for OpenZFS 프로비저닝을(를) 참조하세요.	2022년 1월 27일
콘텐츠 변경: SSPS(자체 서비스 프로비저닝 서비스) 코드 배포.	추가 역할 이름 및 추가 제한 사항은 섹션을 참조하세요 AMS SSP를 사용하여 AMS 계정 AWS CodeDeploy 에서 프로비저닝.	2022년 1월 27일

변경 사항	설명	링크
내용 변경: 링크가 업데이트되었습니다.	끊어진 링크 수정: AMS-AMIs, 설정 찾기, 스택 ID 찾기, VPC ID 찾기, ListVpcSummaries, ListStackSummaries 및 GetStack APIs 예제는 AMS에서 스택 IDs 찾기 을 참조하세요.	2022년 1월 13일
변경된 콘텐츠: Fargate에 대한 EKS 지원	FAQs에 제한 추가: EKS를 사용한 EC2 노드 그룹 생성 또는 관리는 지원되지 않습니다. AMS SSP를 사용하여 AMS 계정 AWS Fargate 의에서 Amazon EKS 프로비저닝 을(를) 참조하세요.	2022년 1월 13일
내용 변경: CloudFormation, DCM(Direct Change Mode)	AmsStackTransform을 사용하여 CF 스택을 생성하거나 업데이트하는 지침이 추가되었습니다. Direct Change 모드를 사용하여 스택 생성 을(를) 참조하세요.	2022년 1월 13일
변경된 콘텐츠: AWS 서비스 이름의 균일성	AMS는 공식 AWS 제목 또는 메타데이터와 AWS 서비스 정확히 일치하는를 참조합니다. 이전에는 패턴 일치를 복잡하게 만드는 사소한 변형이 있었습니다. 예제는 AMS SSP를 사용하여 AMS 계정에서 Alexa for Business 프로비저닝 을 참조하세요.	2022년 1월 13일

변경 사항	설명	링크
콘텐츠 변경: Elastic Container Registry(ECR)의 셀프 서비스 프로비저닝	ECR을 사용하여 사용자 권한을 관리하기 위한 FAQ 항목이 추가되었습니다. AMS SSP를 사용하여 AMS 계정에서 Amazon Elastic Container Registry 프로비저닝을(를) 참조하세요.	2022년 1월 13일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.